UNIVERSITY OF KWAZULU-NATAL

College of Law and Management Studies
School of Management, Information Technology & Governance

THE COMPLIANCE FRAMEWORK FOR THE 7TH POPIA CONDITION IN THE SME ICT SECTOR

A dissertation submitted in fulfilment of the requirements
for the degree of

Master of Commerce
in
Information Systems & Technology

By

Lehlohonolo Itumeleng Moraka
219095366

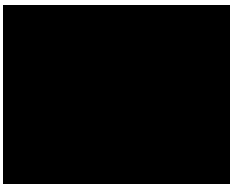
Supervisor
Dr Upasana Singh

2021

DECLARATION

I, Lehlohonolo Itumeleng Moraka declare that:

1. The research reported in this thesis, except where otherwise, indicated is my original research.
2. This thesis has not been submitted for any degree or examination at any other university.
3. This thesis does not contain other persons' data, pictures, graphs, or other information, unless specifically acknowledged as being sourced from other persons.
4. This thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:
   a) their words have been re-written, but the general information attributed to them has been referenced.
   b) Where their exact words have been used, their writing has been placed inside quotation marks, and referenced.
5. Where I have reproduced a publication of which I am author, co-author, or editor, I have indicated in detail which part of the publication was actually written by me alone and have fully referenced such publications.
6. This thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, with the source being detailed in the dissertation/thesis and in the references.



Signed……

Date … 15 January 2022

ACKNOWLEDGEMENTS

I would like to express my most sincere gratitude and appreciation to the following individuals, without whose support it would not have been possible to complete this study:

1. Dr Upasana Singh, in her capacity as my research supervisor, for providing her heartfelt assistance during this complex study, and being patient throughout the learning process.

2. Gill Hendry, the statistician, for meticulously computing and assisting with all statistics in the study.

3. My Grandmother, Naomi Moraka, who has always put me in her prayers.

4. The Moraka family, for supporting me as their son.

5. My friend, Thato Mokhomong, for being a pillar of strength during easy and tough times; and

6. The participants, for assisting, sharing their experiences, and providing the answers to my questionnaire.

ABSTRACT

Data privacy legislation has gained momentum throughout the world and affects users of electronic communication devices in both the private and public sectors. Organisations must adopt data privacy regulations to safeguard data belonging to parties who transact using electronic devices. Furthermore, they need to invest in an organised data privacy solution, such as an information security management system.

POPIA, refers to the Protection of Private Information Act, which is the data privacy legislation in South Africa. The POPIA is a legal document consisting of eight conditions, and the 7th condition in the POPIA speaks directly to information security management systems. The aim of the data privacy legislation is for the government and legislature to give data owners control over their data, which is stored in third-party organisations. The third-party organisations, which store and process the data, must follow strict and mandatory protocols with the aim of protecting the data of a data subject, and using it with the consent of the data subject.

The overall aim of this study is to produce a framework that will assist small and medium enterprises (SME) with complying with the POPIA. Furthermore, it seeks to understand the work done by SMEs in implementing information security by looking at what they do to align with data privacy; to implement data privacy; the resources used for compliance; security threats affecting SMEs; and resources made available for compliance. In the same light, the study looks at existing international data privacy rules and regulations and examines their relationship with the POPIA.

The findings of the study indicate that organisations needed a frame of reference to assist them with implementing the 7th condition of the POPIA. In addition to this, the governments assistance is required by organisations as they implement the POPIA. Moreover, organisations seem to have a fairly knowledgeable structure internally which is resourced and supported by senior management with implementing the POPIA. However, they require external support and validation from government as they are not sure of their efforts align to what the 7th POPIA condition requires. Lastly, the frame of reference is developed by adapting best practice and frameworks which deal specifically to issues indicated in the POPIA 7th condition, and recommendations made by the participants in the study.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

SME:	Small and Medium Enterprises
POPIA:	Protection of Personal Information
GDPR:	General Data Privacy Regulation
ISMS:	Information Security Management Systems
IS:	Information Security
DOS:	Denial-of-service Attack
IT:	Information Technology
IS:	Information Systems
PIPEDA:	Personal Information Protection and Electronic Documents Act
PIPA:	Personal Information Protection Act
PIPITA:	Personal Information Protection and Identity theft Prevention Act
FTC:	Federal Trade Commission
HTTPS:	Hypertext Transfer Protocol Secure
HTTP:	Hypertext Transfer Protocol
DPC:	Data Privacy Controller
PRC:	People's Republic of China
USA:	United States of America
ECTA:	Electronic Communication and Transactions Act
IPA:	Information Privacy Act
IA:	Information Act
IPA:	Information Privacy Act
DPO:	Data Privacy Officer
ECTA:	Electronic Communication and Transactions Act
MICT:	Ministry for Information Communication Technology
CPA:	Consumer Privacy Act
FTC	Federal Trade Commission
ID:	Identity Document
IR:	Information Regulator
SSL:	Security Socket Layer
SPSS:	Statistical Package for Social Sciences

CHAPTER 1: INTRODUCTION

1.1 Introduction

The Protection of Personal Information Act No. 4 of 2013 (POPIA) is a legal act passed by the South African government (Staunton et al., 2019). The aim of the (POPIA) is to protect people's personal information processed by private and public organisations in the Republic of South Africa (De Stadler & Esselaar, 2015). The POPIA establishes a set of conditions for managing personal information and regulates the transmission of information. The focus of this research is to develop a compliance framework for the 7th condition of the POPIA, which covers the security safeguards and technical measures organisations need to adopt to be compliant with the POPIA.

The POPIA was created in response to issues associated with information privacy (Information Regulator, 2013b). People's personal data are processed and used for various legal and illegal activities. Therefore, the South African government has legislated the POPIA to address how personal information is managed (Information Regulator, 2013b). An information regulator was appointed by former President Jacob Zuma in order to have a legal body oversee POPIA issues, such as data breaches; assisting with POPIA implementation and training; investigating data breaches; and receiving data complaints from subjects affected by data breaches (Information Regulator, 2013a). The aim of this research is to develop of frame of reference for POPIA compliance in the SMEs, e-commerce ICT sector, and to explore how SME manage data privacy legislation.

1.2 Background of the Study

Processing and disseminating personal information form part of the current digital transformation (Staunton et al., 2019). Therefore, protecting information has become a very important aspect when managing information. Public and private organisations collect and process personal information belonging to different entities, such as people and businesses. The information processed comes from various organisations and includes information such as, but not limited to, healthcare records; physical addresses; employment details; or any form of information that may identify a specific person (Gratton, n.d.).

Organisations which process information without the consent of the owner are in breach of the POPIA (Ablon, Heaton, Lavery & Romanosky, 2016). Institutions that process and disseminate private information must comply with government regulations in protecting confidentiality, accessibility, and being accountable for any information processed.

Although the POPIA is not yet fully implemented, it is very important for public and private organisations to start planning for compliance. The 7th condition of the POPIA is written in a legal

format and cannot be useful on its own. Organisations will therefore need to follow existing best practices and standards to address the limitations of the 7th condition in the POPIA. Part of this study is to develop a framework for the 7th condition of the POPIA by using an existing information security theoretical framework and adapting it to an existing conceptual framework. Furthermore, it will add additional components to complement the missing parts so that there is a new, complete framework for the implementation of the 7th condition of the POPIA.

1.3 Research Problem

The aim of the POPIA is to regulate how personal information is processed by public and private entities (Ablon, Heaton, Lavery & Romanosky, 2016) . It is the duty of both private and public organisations to ensure that they are compliant with the POPIA (Information Regulator, 2013b).

The 7th condition of the POPIA document does not include a technical guideline or a frame of reference that private and public organisations can adopt as a guide to be compliant with the POPIA. This makes the POPIA processes cumbersome for organisations to follow while attempting to align to the requirements stipulated int the regulation (South Africa - Data Protection Overview, 2021).

A well-written technical guideline for the 7th condition of the POPIA would make it easier for organisations to implement the POPIA and fulfil its requirements. Moreover, it is practically impossible for organisations to be compliant with the POPIA without a proper guideline in place. Businesses which do not implement the POPIA are in breach of the law and stand the risk of being fined or imprisoned. Furthermore, if organisations are not provided with the necessary resources to implement the POPIA, they automatically inherit data-related vulnerabilities. Consequently, the organisation is at risk from hackers and may find their data integrity, and business reputation, compromised.

SMEs in the E-commerce sector store customer personal data, such as contact numbers and physical addresses (OECD, 2011). Such data can be exploited by cybercriminals for various crimes such as identity theft or sending unsolicited spam emails or SMSs to the customers. It is for this reason that a framework for implementing the 7th condition of the POPIA is necessary for public and private organisations to be compliant with the POPIA. Lastly, this research seeks to use existing, tried-andtested international standards and frameworks, such as the ISO and COBIT 5, to develop a framework that can be adopted by public or private bodies in implementing the 7th condition of the POPIA. Organisations that implement the POPIA inherit a good relationship with customers, maintain a healthy business reputation and expand their potential for business and financial growth in business.

1.4 Research Questions

1. What is the POPIA’s impact on information security?

2. How do employees in different functions in the SMEs implement the POPIA?
3. What are the challenges of implementing the POPIA?
4. What are the benefits of implementing the POPIA?
5. What are the repercussions of disregarding POPIA?

1.5 Research Objectives

1. Outline the POPIA and information security.
2. Investigate how employees in different functions at SMEs implement the POPIA.
3. Identify the challenges of implementing the POPIA.
4. Identify the benefits of implementing the POPIA.
5. Identify repercussions of disregarding POPIA.
6. Develop a framework for implementing the 7th condition of the POPIA.

1.6 Significance of the Study

It is prudent to reiterate that the POPIA is a legal document and does not provide any specific technical guidance for organisations to follow to comply with the 7th condition of the POPIA. Furthermore, the Protection of Personal Information Act requires organisations to put resources into their information security management systems, and this is a technical requirement. The study produces a frame of reference for organisations to use for implementing the POPIA. The frame of reference provided by this study is based on the existing internationally recognised standards and frameworks for information security management. Thus, it provides a reputable POPIA framework using internationally recognised policies and frameworks.

The study can make South African organisations aware of the importance of information privacy legislation and provide an indication of how to implement the 7th condition of the POPIA. The results of the findings in this study should allow organisations to be prepared for the implementation of the POPIA.

If the study were not conducted, organisations would have limited information on how to implement the POPIA. Furthermore, they might not recognise the urgent need to start preparing their information security management systems so that they align with POPIA. This study also serves as a reference to the information regulator to assist organisations with implementation.

1.7 Research Approach

For a conclusive study giving the best interpretation of the results, and an understanding of the phenomenon being studied, a quantitative research approach was adopted. The quantitative research

approach was chosen because it enabled a detailed investigation for the development of a frame of reference that would aid POPIA implementation in SMEs. Furthermore, it provided us with an exhaustive process to achieve the objectives of the study.

A questionnaire was the primary, and only, data collection tool in this study. For this study, data was collected through a self-administered questionnaire, and the questionnaire was electronically distributed by the researcher. A quantitative research approach suited this study. A quantitative approach is an objective, systematic, formal procedure of describing and testing relationships to examine causality and effect between variables (QuestionPro, 2018).

1.8 Research Design

The primary aim has been to develop a framework for the 7th condition of the POPIA. A descriptive survey was adequate for this study because it yields an accurate portrayal of the opinions; abilities; beliefs; characteristics; and knowledge of the population surveyed. The data was only collected by means of a questionnaire, and it was the primary data. The survey was sent to the participants electronically to determine their POPIA understanding and to collect information that would assist in developing a framework for the POPIA 7th condition. The study aimed to find IT practitioners in the ecommerce SME space who were working on developing the e-commerce site and were tasked with overseeing the end-to-end systems security and compliant technical measures for the e-commerce site.

1.9 Study Site and Target Population

Gauteng is the province with the biggest in-migration from other South African provinces. It offers more employment and business opportunities, and it has the most economic square metres in Africa. The population is estimated at 15.7 million, and it is the smallest province in South Africa (Rogerson, 2018). The population for this study was specifically in Johannesburg and Pretoria, the two major cities, where the sample with the required skills are generally known to be located. Furthermore, the researcher resides in Gauteng and has greater access to the sample. Gauteng is also known as the economic hub of South Africa and houses many professionals from different sectors. Therefore, it was easier for the researcher to reach the sample.

The targeted population of this study included information technology practitioners who are involved in the information security aspect in South African small and medium enterprises. These practitioners operate from the e-commerce IT Sector. These experts were able to provide feedback that met the objectives of the study and were within the researcher's reach. In addition, the information technology practitioners make up the team that needs to be technically involved in implementing the POPIA and building systems used by the organisations. This population was also easy to access because SMEs do

not have as many restrictions as large corporate organisations, which could have delayed or prevented the researcher from conducting the study.

1.10 Sampling Method

Sampling refers to the process of selecting a portion of a full population (William, 2016). The portion must represent the actual population from it was extracted. This process is referred to as generalisation (William, 2016) and allows the researcher to gather information that meets the objectives of the study. Simple random sampling is the process of randomly selecting a sample from a population, with the intention of giving everyone in the qualifying population a fair chance to participate in the survey.

According to Jorge Faber (2014) a bigger sample reduces variations and increases the chances for the research to yield a more accurate outcome. Researchers, in general, may be biased when determining a sample size, and in measuring or choosing a healthy and significant sample. For example, when they estimate the population size for an area of research of interest to them, they pick regions where the sample is will best address their research interest, rather than giving the entire population the same probability of being selected (Jorge Faber, 2014). To reach a more precise estimate of the population size, the numbers selected for the sample in any area must be in proportion to the total size of the population. A simple random sample has the benefit of reducing bias and giving all the participants an equal opportunity of participating in the sample (Horton, 2020). The selection of areas to be sampled in a simple random sampling can be facilitated by a random number generator. These random number generators can generate a random list of numbers indicating participants or places to sample.

The roles of the employees, or consultants, were closely associated with the development of the actual e-commerce solution and included software engineers; database developers; information security specialists and data controllers. To reinforce the sample's validity, the sample was informed on the POPIA legislation in general and had to have detailed knowledge on the 7th condition of the POPIA. This ensured that the researcher achieved the objectives of the study.

1.11 Data Collection Method

The researcher used a questionnaire as the main data collection instrument for this study. The questionnaire was designed in a way that addressed the objectives and questions of the study. Various information technology (IT) practitioners selected in the sample were required to fill in a questionnaire. The questionnaire was aimed at collecting information from the professionals in South Africa who are involved in implementing the POPIA/information privacy. The questionnaire was distributed electronically, and participants were requested to complete and return the questionnaire within a specific time. A questionnaire was an appealing approach due to the following:

1. They ensure a higher response rate.
2. The researcher collects them personally.
3. They give an element of anonymity.
4. Administering a questionnaire is not too taxing.
5. There is a less likelihood of bias.

1.12 Data Analysis

This research used closed-ended questions. The data analysis used in this study is expanded on, below. The researcher employed a statistical data analysis computer software package named Statistical Package for Social Sciences (SPSS). The data was analysed using descriptive statistics, which is the process of analysing data without the intention to generalise. Various diagrams, such as bar graphs, were produced from frequency tables. The data collected was cleaned and loaded into the SPSS software.

1.13 Limitations of the Study

The study findings can only be applied in areas from where the study sample was selected. Furthermore, due to budgetary and time constraints, the researcher was not able to add other business sectors (hospitality, tourism, medicine) into his study. Therefore, the study is limited to sectors from where the sample was selected. Lastly, the framework developed in this study is a high-level framework, and organisations would need to invest in buying the ISO 27001/ 27002 and COBIT 5 for information security packages, in order to access the deeper level guide.

CHAPTER 2: STRUCTURE OF DISSERTATION

2.1 Chapter 1

This chapter introduces the background of the study. In addition, it describes the research objectives, problem statement, research problem and research questions which the study aims to answer. Furthermore, it indicates the rationale for conducting the study, and briefly discusses the methodology adopted for this study.

2.2 Chapter 2

This chapter shows the structure and flow of the dissertation.

2.3 Chapter 3

This chapter gives a full review of the literature on information security; information security management systems; SMEs; e-commerce; and data privacy legislation, locally and globally. In addition to this, several key concepts and definitions that are used in this study are discussed. In this chapter, the researcher also elaborates on the importance and drawbacks of implementing data privacy legislation. Finally, the theoretical and conceptual framework which is used to guide the empirical stage of the research is outlined.

2.4 Chapter 4

This chapter covers the research methodology applied in this study; as well as the process adopted in data collection; the sample selection; the population from which the sample was drawn; and the instrument used for collecting data. Lastly, the chapter outlines the data analysis strategy used in the study.

2.5 Chapter 5

In this chapter, the data collected in the empirical stage was analysed extensively using descriptive statistics. Output tables, graphs and frequency tables are shown and are used to explain the data. The data all aligns with the questions asked in the questionnaire stage of this study. This data then addresses the objectives of the study. Key components in this chapter are later incorporated into the framework development stage.

2.6 Chapter 6

This chapter discusses the findings of Chapter Four, summarises the main conclusions, indicates the limitations of the study, and makes recommendations.

2.7 Chapter 7

In this chapter, the proposed framework for SMEs to use as a guide in implementing the 7th condition of the POPIA in the IT e-commerce sector is shown and explained in detail.

2.8 Chapter 8

This chapter outlines the summary and major conclusions reached during the study, including the discussion, and findings from Chapter Four. It concludes by providing recommendations on future research work.

2.9 Conclusion

The researcher has provided the reader with a detailed overview of the research work, which elaborates on data privacy legislation; information security; information security management systems; ecommerce; and data security. In addition to this, a definition of the problem statement, research problem, limitations and research questions were outlined.

CHAPTER 3: LITERATURE REVIEW

3.1 Introduction

This chapter begins with introducing information security and the general components of information security. In addition to this, it defines SMEs, and then goes on to cover data privacy legislation. Furthermore, the chapter reviews the literature that covers data privacy legislation at the global level, local data privacy issues, and information security management systems that are internationally recognised. Lastly, the chapter introduces the theoretical and conceptual framework that guides the study.

3.2 What is IT security and its components?

Information security refers to a situation where an information or data asset is quarantined from unauthorised access, tampering, and distribution (Fruhlinger, 2020). Data refers to a combination of numbers, symbols, and characters which are stored and processed by a computer and result in information when processed (Bridgwater, 2018). Cybersecurity refers to measures taken to protect information from illegal access. This may be achieved by employing both software and hardware products which are designed to secure data, e.g., antivirus software, but not limited to virtual private networks (Kaspersky, 2020). Information technology security, also known as IT security, refers to a process of applying cybersecurity methods and practices to achieve information security (Cisco, 2016). As a result, the aim is to achieve integrity, confidentiality, and availability of an information asset, while preventing intruders from accessing the information.

IT security developed as a subfield within the information technology industry. Its focus is to ensure that there are key skills and resources to oversee the protection of information and data in public or private organisations (cyberinsiders, 2019). Organisations generally have an information technology division overseeing the information security tasks, using information security practitioners (cyberinsiders, 2019). However, some organisations have the information security division as a separate unit (cyberinsiders, 2019). There are several roles assigned to information security, and they aim to safeguard an organisation's information asset holistically (cyberinsiders, 2019).

3.3 The justification for investing in information security.

Information security is achieved only when an organisation or individual employs IS security measures (Tumber, 2019). These measures may require technical or physical resources. The physical resources may be locks, doors and/or computers. The logical resources may be software solutions designed to secure information assets (Tumber, 2019). Public and private entities are required to have successful information security (Tumber, 2019). The information secured would generally belong to customers

and other stakeholders who are involved in an organisation's operations: this could be municipal account information belonging to homeowners in any given location. The data could be financial or personal, and such data must be protected from illegal access and modification. If an organisation's data are compromised, it may lead to financial loss, and a damaged reputation (Tumber, 2019). Therefore, it is necessary for organisations to have measures in place to protect their information assets. The protection of information requires a financial resource and support from an organisation's top-level management (Wang, 2019). The financial resource should be utilised to employ an information security team, and procure physical, and logical, IT security assets (Wang, 2019). The implementation of a successful information security system is fully dependent on supportive top-level management for resources and IS strategy implementation.

3.4 What is E-commerce?

The internet has become a focal point for consumers to acquire goods and services. Consumers find it convenient to buy and sell services through the internet. The internet enables consumers to access a wide range of products and services electronically, by using handheld devices, laptops, and computers (Amin, Kansana and Majid, 2016; Guide, 2020). The process of acquiring and selling goods and services through the internet is referred to as e-commerce (Amin, Kansana and Majid, 2016).

E-commerce transactions are all electronic and require the end-user to be connected to a network. These transactions occur on the internet and data gets transmitted. The data transmitted can be personal information, financial details and, possibly, address information. These details are required because a vendor selling on the e-commerce platform needs to deliver a product or service to a specific customer at a specific location (Accenture, 2019). The customer may be expected to use a card or their banking details to acquire the products or services of their choice, sold by a vendor online. The card details belonging to the client are sent and processed by a server (Accenture, 2019). This transaction is referred to as an e-commerce sale.

In South Africa, there are multiple e-commerce businesses which do not have physical stores, as well as businesses that operate online, but which also have physical storefronts for customers to walk in and purchase goods and services. However, in recent years, consumers have tended to be more reliant on ecommerce platforms for purchasing goods and services (Amin, Kansana and Majid, 2016; Ngalonkulu, 2019; Guide, 2020). As a result, most business sales are driven by e-commerce transactions, and more businesses are investing in their own e-commerce platforms (Amin, Kansana and Majid, 2016; Ngalonkulu, 2019; Guide, 2020).

E-commerce platforms are generally web-based applications or mobile applications. The mobile and web-based applications are used for accessing the products and services belonging to businesses

virtually (Accenture, 2019). E-commerce applications operate locally and globally. In South Africa, well-known platforms are Takealot.com, and Wish.com.

3.5 What are SMEs?

SMEs refer to small and medium enterprises. These are generally small organisations with a staff complement of 50 or less, and which operate within a specific geographical area (Fatoki et al., 2011). These organisations have fewer financial resources and provide products and services on a smaller scale (Fatoki et al., 2011). SMEs are vital in the economy as they play a crucial part in entrepreneurship and employment creation, thus making it possible for the economy to grow (Fatoki et al., 2011). SMEs, just like any other business, are subject to rules and regulations that affect the country they operate in (Berry et al., 2002). Therefore, SMEs must be capable of adopting any legal requirements imposed by the country they operate in. In addition to this SMEs also include medium size businesses.

3.6 What is E-commerce & IT security internationally, in Africa and in South Africa?

E-commerce, as described above, is where the buying and selling of products happen online. Ecommerce transactions are prone to challenges, including data integrity, meaning that the data processed during an e-commerce transaction may be tampered with (Kraft & Kakar, 2009). Furthermore, the confidentiality of the data processed is affected (Berry et al., 2002; Kraft & Kakar, 2009). Moreover, the availability of the data in the e-commerce transaction is exposed through the system and may land in the hands of individuals who should not have access to it. As a result, information belonging to buyers and sellers on e-commerce platforms is used for activities for which it was not intended. This includes marketing; stealing of banking information which results in theft of money; and exposing residential information and compromising the information belonging to the buyer and the seller (Kraft & Kakar, 2009). Therefore, it is paramount for e-commerce transactions to be secured from end-to-end. This requires organisations who invest in e-commerce applications to ensure that their systems are secure from intruders (Abraham, 1999). There are companies who develop software to secure IT systems and deter illegal activities that will compromise the health of their e-commerce systems.

There are several online stores which operate locally and internationally. Amazon.com is an online marketplace which was founded in the USA and employs over 750 000 employees (Amazon, 2018). Amazon.com started with selling books, but later expanded its offering to include electronics, and then computers; games; furniture; food; streaming services; and jewellery, to mention a few (Amazon, 2018). Amazon is the second largest employer in the United States of America. Amazon, through its ecommerce business, generates over $410 000 000 daily, which is estimated at $17 000 000 every hour (Amazon, 2018). This indicates that multiple transactions are processed on e-commerce systems.

South Africa has an online marketplace named Takealot.com. It is the most innovative e-commerce organisation in Africa, and the largest e-commerce retailer in South Africa (Takealot.com, 2019). Takealot has acquired warehouses within the major provinces of South Africa and delivers goods and services directly to the doorstep of their customers. Takealot ships 80 000 items per day during peak periods, and 35 000 items per day on average (Takealot.com, 2019). Jumia is an Amazon and Takealot equivalent but operates in certain African countries on a much smaller scale. Jumia is expanding its operations throughout the African continent and provides a wide range of items such as fashion clothing and electronics (Jumia Group, 2020).

African e-commerce businesses are few, but there are many e-commerce partners operating in Europe and Asia, such as Alibaba.com. This shows that e-commerce has grown rapidly and it is growing globally (PayGate, 2017). As e-commerce transactions escalate, hackers and other intruders have a growing market to target. This means that information belonging to customers may be compromised. There are certain IT security standards which are mandatory before an online platform is fully deployed into the market (PayGate, 2017). These security standards vary in complexity and level of protection. Encryption is the process of scrambling text into an unreadable format so that it does not make sense to an intruder accessing the data. Encryption is delivered by an algorithm designed to make data transmitted through the server unreadable (Encrypt, 2017). HTTPS (HyperText Transmission Protocol Secured) refers to another data transmission rule applied to a website. HTTPS is designed to ensure that the data transmitted on the server has integrity and confidentiality. Encryption and HTTPS are elements of IT security, or cybersecurity to be specific (Kothari, 2019). These are measures which are in place to ensure that IT systems are a safe place for customers to share their personal and banking details.

Type text here

Cybersecurity ensures that transactions that happen in e-commerce systems are secured (Kaapu & Paakki, 2006; Kothari, 2019). However, the strength of the security in an e-commerce site is dependent on the financial investment made by the organisations that own the e-commerce applications (Kaapu & Paakki, 2006; Kothari, 2019). Web-hosting companies sell domain names and web server space to organisations that operate e-commerce applications (PayGate, 2017). They are third-party companies that are given access to data transmitted by the e-commerce customers and vendors (Grid, 2018). Therefore, it is vital for e-commerce business owners to specify their cybersecurity policies, thus ensuring a certain level of understanding between the stakeholders involved with their online business. This could be the adoption of SSL certificates/HTTPS, or encryption standards. In South Africa, there is an organisation named Afrihost which is partially owned by MTN, the local telecommunication giant. They store databases and web pages, together with code logic, for a certain percentage of the ecommerce market. If organisations wish to buy webspace from Afrihost, they may communicate with the IT security team there and assess whether the information security policies from Afrihost align with their

own policies. The same applies to all organisations that wish to have an IT system hosted externally. However, certain organisations may choose to have their IT systems hosted in-house, which gives them physical and logical control over them (Grid, 2018).

E-commerce websites also use additional third-party organisations for sending/receiving payments online (PayGate, 2017). These organisations are called payment gateways. They work with merchants and banks to send/receive payments electronically. Payment gateways specify certain requirements before giving e-commerce businesses access to receive payments on their websites (PayGate, 2017). Such requirements include terms and conditions, where the owner of the website specifies their electronic use consent, which must be agreed to by any party purchasing goods or services from their e-commerce site (Rieck, Korolev & Barker, 2008). These terms and conditions inform the customers about the data transmitted by the site and the potential risks associated with this (Rieck, Korolev & Barker, 2008). Therefore, customers are aware of the risks associated with transmitting their details on the websites. Some e-commerce has password policies which guide users to use complex passwords that are more difficult for hackers to crack.

3.7 Incidents that happen on e-commerce sites

E-commerce sites have grown significantly on a global and local scale. This is because most opensource sites make it easy to set up e-commerce businesses (Kumar, 2019). This is good for business in general. However, at the same time, it has created a lucrative target for spammers, hackers and malicious agents who pose a security risk for the e-commerce business (Kumar, 2019).

For e-commerce businesses to defend themselves from security risks, they need to have deep financial resources, and this is a challenge for smaller companies who cannot afford it (PixelPin, 2018). Therefore, smaller online businesses become the most vulnerable. This does not only affect e-commerce businesses, but all online-based systems (Forde, 2015). In one incident, hackers were able to access over 227 e-commerce sites and insert advertisements into them (Kumar, 2019). Moreover, there is a huge underground market in phishing, denial-of-service attacks, spamming, and fraud (Kulakov, 2019).

With the increasing sophistication of attackers in a connected world, massive data breaches have been found in e-commerce sites, and more than ever before (Kumar, 2019). Whilst there are many symptoms, the list below summarises a few of the signs that an e-commerce site has been compromised (Lacey & PaulSalmon, 2015):

- the same IP address making repeated requests on the server, thus adding load to the site;
- bots that are designed to choke the bandwidth;
- foreign products listed for sale on your site;

- a breached database;
- unknown active administration user accounts appearing on the database;
- customers reporting that their credit information has been stolen, despite having put security measures in place;
- new or unknown database tables appearing on the site;
- customers complaining that they had paid for an order for which the vendor did not receive any payment;
- multiple pages with advertisements appearing on your website without your consent or knowledge;
- brute force attacks;
- Google or the hosting provider blacklisting your website;
- customers complaining about being redirected to other sites while busy on your website; and
- suspicious advertisements popping up, requesting users to install components or plug-ins into computers.

The list above identifies some of the symptoms of compromised e-commerce sites. It is prudent that measures are in place to secure e-commerce sites from attacks.

3.8 Common security and data privacy vulnerabilities associated with E-commerce sites.

SQL injection is a threat that is posed by hackers to gain entry into an e-commerce site's database to violate the sensitive information such as credit card information or transaction histories; and sometimes they steal the whole database and sell it to marketing companies (Tomlinson, 2009). Hackers may also change the pricing of products sold on the site, add discounts, and make items free. This basically gives the hacker the privileges of the site owner.

Cross-site-scripting happens when an attacker inserts scripts into an existing site (Tomlinson, 2009), thereby attacking an active user who is busy on the e-commerce site. The attacker may steal information or inject different content into the site. This hacker may compromise the administrative users of a site and create havoc.

Bad-bots are scripts designed to perform a specific task and report back to the master bot (Tomlinson, 2009). These bots could steal pricing information for competitors to gain a competitive advantage (Suchacka, 2020). According to Suchacka (2020), 21% of e-commerce users are affected by bots (Suchacka, 2020). Bandwidth choking is a type of bot used by hackers to put a spike in an ecommerce website, more specifically during peak sale hours. This results in a slow website that behaves unreliably for the buyers (Suchacka, 2020). As a result, the buyers lose interest, and the vendor loses revenue.

Content scraping is an attack by bots to steal content data from an e-commerce site, with the intention of gaining competitive advantage (Suchacka, 2020).

Malware is a program designed to spread throughout an e-commerce site with the intention of skimming credit card data or encrypting databases and blocking administration from accessing a site (Regan, 2017). Research informs us that malware has harmed over 7000 e-commerce sites in less than six months (Regan, 2017). This malware is dubbed MagentoCore, which is aimed at affecting Magento-based online stores. Magento is a business that sells e-commerce sites. Denial-of-service attacks are generally launched by competitors who hire cybercriminals to reduce a competitor's revenue and increase their own presence in the e-commerce space (Rubin, 2011). Peak business days like Black Friday attract a lot of denial-of-service attacks (Rubin, 2011). E-commerce businesses must be proactive, or they lose revenue.

3.9 Methods to deter IT security risks.

Hackers always find ways to attack systems and steal data (Sadler, 2015). Therefore, it is vital that organisations implement disaster management strategies to prevent attacks from hackers (Sadler, 2015). Some attacks may take a time to repel, but business continuity is crucial for the survival of the business. Businesses should put an effort into protecting their online stores.

It is evident that there are groups, or individuals, who seek to maliciously damage e-commerce sites (Sadler, 2015). Furthermore, e-commerce sites are hubs for online payments (Zadig, 2010). Cybersecurity and IT security can be employed to reduce these risks (Zadig, 2010). Payment card industry regulation compliance (PCI) is a set of industry-based regulations for transmitting financial information over an e-commerce website (Kagan, 2015). These regulations limit how financial data is managed by e-commerce sites. They require that financial information is not stored on a database, or by a local server (Kagan, 2015). PCI-compliant e-commerce sites are usually trusted by customers and grow, thus increasing their revenue. Content delivery networks (CDNs) are useful for organisations during peak buying times, like Black Friday (Skrba, 2019). They are capable of controlling web traffic to the site, and the modern ones are capable of monitoring site performance, managing traffic overload and increasing the performance of a website (Skrba, 2019).

Hypertext transmission protocol secured (HTTPS)/ SSL is a certificate usually issued by a third-party company that sells security certificates for transactions over e-commerce sites (Skrba, 2019). These standards ensure security for online transactions. Conducting updates and security audits on the site is essential, given the sensitivity of information that flows on e-commerce sites (Varghese, 2020). Audits can yield information that would have given hackers access to the sites. These audits assist the ecommerce business in finding active ways to avoid hackers (Varghese, 2020). Security audits indicate

loopholes on the e-commerce sites, and when loopholes are identified, patches and updates must be implemented so that the security risks are avoided (Varghese, 2020).

The SME sector is challenged with complying with IT security rules and regulations, or what they refer to as 'red tape' (Supplied, 2018). Such rules and regulations come partly from the government, but also from the private sector. Depending on the customer base of these SMEs, some may be required to comply with international regulations (Supplied, 2018).

All South African-based SMEs are affected by the POPIA, regardless of size (Pillay, 2014). Therefore, e-commerce SMEs must seek assistance with complying, or they may end up paying heavy fines; gaining a bad business reputation, and going out of business (Botha et al., 2015). SMEs in e-commerce generally operate with few, or no, financial resources, and this makes it a challenge for them to adhere to legislation that requires money to be implemented (Botha et al., 2015). The South African POPIA regulations require compliance from all levels and sectors of businesses, as e-commerce is exposed due to the type of information supplied through online transactions (Botha et al., 2015).

3.10 Below is a list of the 8 conditions stated in the POPIA (Information Regulator, 2013a).

3.10.1 Accountability

The responsible party must put the POPIA into effect, this means ensuring that measures are in place for POPIA compliance, and being accountable for any POPIA-related breaches. In respect of ecommerce platforms, accountability means that the business is accepting responsibility for any violations of the act. Failing to implement the POPIA may result in imprisonment or heavy fines. Lastly, an organisation is accountable for collecting and processing the customers' data, and how it shares it with third party organisations. These are the steps that ensure that adequate measures are considered, from top-level management to bottom-level company operations. The organisation must have internal processes to implement the POPIA.

3.10.2 Processing limitations

Personal information must be processed legally, and the owner of the information must consent to any information processed. The information must not be processed beyond what the owner of the information has agreed on. In the e-commerce environment, data is collected to provide a user with the basic functions necessary to log onto the platform in order to purchase goods and services, and accept delivery of them. In this regard, personal information is exposed. If the organisation violates the terms which the user has agreed to, then they have gone beyond the processing limitations agreed upon by the customer, and this may lead to legal violations and fines. Lastly, if customer information is shared with

third party businesses, the business must make sure that the customer is informed and agrees to such conditions.

3.10.3 Purpose-specific

Information can only be processed for legitimate reasons, and those reasons must be specific and legal. In an e-commerce environment, the customer must be informed of the reasons for their data being collected. If an organisation agrees to collect a customer's personal address to deliver goods purchased on its site, it must specify this information clearly to the customer. This information might also include how long the customer's records will be kept before being destroyed. This assures customers that their data is collected for legitimate reasons. This level of transparency does not only limit businesses, but also increases customer confidence when sharing personal information to online businesses.

3.10.4 Further processing limitations

A) The processed information must not be processed for secondary reasons unless the processing is linked to the original reason. In the e-commerce business, further processing limitations are also communicated to the customer, or owner of the data. This ensures that the customer is aware of, and agrees to, any other use of their data. This could be reusing their information to promote products and services from other business units. If a business plans to retain a customer's records for three years, it must inform the customer what they plan to do with the data for the entire duration. POPIA refers to the customer as the data subject; thus, the data subject must be aware of any extra processing limitations on data provided to businesses. In short, the information cannot be used for anything beyond what it was collected and intended for.

B) Information quality: The responsible organisations must ensure that the information they are processing is updated, accurate, and not misleading. The accuracy of such data can be validated by the data subject. Furthermore, if it is not possible to validate the accuracy of data from an IT system, it is important that the data gets sent back to the data subjects so that they can validate it. Such information can be as simple as address details. Businesses must follow the guidelines within the POPIA and adopt the correct processes for validating data. This can be done by email, SMS, and phone call. In addition to this, the data subject must be informed why the data needs to be validated, including how and why it will be used. Data quality is key in driving business operations for the e-commerce sites, to ensure that they deliver goods to the correct address and send communication to the correct recipient. Data which is only collectable by paper can be validated with the data subject once it is captured electronically.

C) Openness: The owner of the information processed must be informed of, and agree to, the processing of their information. The data collector must prove that they have consent from the data subject to process the data given to them. Furthermore, the data subject must be informed of processes they can follow in the event they want to remove the data stored by the businesses; for example, how to opt out of receiving emails from the business. In addition, the data subject must be informed about ways to report the data collector if they believe that their data is being used for more than what is intended. So, in e-commerce businesses, the data subject must be informed who to contact, if they want to have their data removed; and they need to be advised on routes they can take if they suspect that the data has been misused. In this regard, the data may reside in the database of the e-commerce business, but the owner of the data has the power to decide how their data is used and can be given access to the data if they request it.

D) Security safeguards: Personal information must be kept safe against the risk of unlawful access, loss, modification, disclosure, and destruction. This requires the entity processing the information to ensure integrity, confidentiality and accountability. These pillars of the POPIA legislation require technical ability from an organisation. Therefore, certain specialists must be employed or deployed to ensure that the business applies the measures in this section of this legislation. In an e-commerce environment, data privacy levels can be implemented by means of data encryption. This means that the data collected from the users must be scrambled and turned into an illegible form, so that the data cannot not be easily translated if it is exposed. Furthermore, a safe browsing environment must be employed. The e-commerce system must have security protocols that certify that the data transmission between the data subject and the system is secured end-to-end. This process requires a financial investment. The security safeguard level needs to be implemented for protecting customer information. Therefore, it is critical to protect the reputation of the business through employing measures to secure customer information. When data is leaked or hacked, it means the technical security implemented by the organisation has loopholes which need to be fixed. Technology and technical security systems are easily compromised when they are not updated. Therefore, the business must implement security safeguards in a proactive manner, enabling them to improve on known threats, thus deterring data privacy violations and meeting the POPIA legislation requirements. The challenge with the POPIA is that it does not specify what entities need to do to satisfy the requirements of the 7th pillar.

E) Data subject involvement: The owners of the data may request that their information be deleted or may require details on how their information is processed and stored. Therefore, unless stated otherwise, the owner of the information has the right to cancel information processing activities. The data subject cannot be charged for requesting the full details contained by the processing

organisation. This information must be given to the data subject, including a full description of it. The data processing organisations are mandated with the responsibility of ensuring that they have processes in place to give the data subject valid and correct information. The only requirement from the data subject is to prove that they are the owner of the data being requested. Lastly, the organisation must be fully transparent to the data subject and involve them when requested.

3.11 Current personal information breaches by organisations and weaknesses in their information security management systems.

According to an article published by the Sunday Times newspaper, there have been reported data leaks of the almost one million people who pay road traffic fines online (Gous, 2017). The data leak contains 934 000 records with ID numbers, email addresses, passwords, and full names of customers (Gous, 2017). This data was claimed to have been leaked by one of the companies who are responsible for collecting payments for vehicle traffic fines online. Furthermore, the information regulator was informed about the leak (Gous, 2017).

According to Gous, the information regulator is sitting with more than 300 reported data privacy breach cases, which require action (Gous, 2017). Therefore, it is imperative to achieve compliance with POPIA at an early stage. In early 2018 Facebook indicated that more than 87 million user records had been improperly shared with Cambridge Analytica, and 60 000 of these records belonged to South Africans (Gous, 2017). In late 2017 there was a data dump which revealed personal information such as national ID numbers, contact details and addresses of prominent people, including the president of South Africa at the time. Furthermore, it was reported that a prominent real estate firm had admitted to having hacked data belonging to customers (Gous, 2017).

POPIA research conducted by Dala within South Africa, involving 167 participants, has revealed that less than 50% of organisations in South Africa understand what POPIA is (Dala, 2017); while over 24% have a fair understanding, and just over 10% have a good understanding of the POPIA. Therefore, the level of compliance with the 7th condition of the POPIA is weak: Dala's findings show that 16.2% of organisations are implementing the full security safeguards; while 7.2% are unsure about how far their implementation of confidentiality, integrity and compliance of electronic personal information has progressed. Some 6% of organisations are not sure of their POPIA compliance (Dala, 2017). Moreover, only 48% of the 167 participants in Dala's findings have made a formal undertaking to implement security safeguards or to have a formal POPIA in place. The most important consequence of noncompliance with the POPIA is reputational damage (Dala, 2017). Such damage has the potential to reduce the revenue of an organisation and affect its share price dismally.

If an organisation is found to have been in breach of the POPIA they are required to report such a breach to the information regulator; and having done so, they should also inform the affected parties within a specific time period which will be advised by the regulator (Information Regulator, 2013b). Organisations must update their information security management systems regularly to achieve confidentiality and integrity of data.

3.12 Security breaches in South Africa

The POPIA is not yet fully implemented. The information regulator to enforce POPIA has been appointed (Ian Jacobsberg, 2019), but with limited powers in this regard. Furthermore, organisations who are in breach of the POPIA will continue to operate with little or no sanction (IS News, 2020). However, South Africa has seen many data privacy and security violations in different business sectors. Whilst this research is focused on the e-commerce industry, the POPIA applies to all the business and government entities in South Africa.

The number of devices used to access data have increased, and different devices have different operating systems and security measures (Strachan, 2008). The security of data repositories belonging to businesses is affected because they are faced with challenges of preventing data breaches that can come from numerous sources. This can be dependent on device operating systems and security measures (Andress, 2014). It is challenging for businesses to secure devices which are not stored in their asset register (Andress, 2014). However, every organisation must have data privacy measures in place (Ian Jacobsberg, 2019). Furthermore, given that businesses are currently faced with an ever-evolving information system environment, business leaders must ensure that they have adequate proactive measures in place to meet the IT security challenges that occur during these times (Ian Jacobsberg, 2019). This involves a stringent risk management approach and also educating customers on data security. This can be achieved by sending customers emails, SMSs and other communication containing tips on protecting their accounts, changing their passwords regularly and not sharing login information (Kandeh, 2018).

Liberty Holdings is a financial services-based organisation with a large business footprint within South Africa (Gernetzky, 2019). Liberty has a life insurance unit called Liberty Life, which had a massive data breach where over 30 million customer personal records were leaked online (Niselow, 2018).
Liberty provided limited information about the nature of the breach (Niselow, 2018), but it is understood that the email repository of the organisation was hacked (Magubane, 2018). This led to the exposure of customer personal insurance information. Liberty informed all its clients via SMS about the security breach and sited it as a ransomware (Moyo, 2019). Reports inform us that the Liberty data breach is the biggest data breach to ever have occurred in South Africa (Shapshak, 2018). It has also been reported

that data breach incidents have been increasing and companies must strengthen their data privacy systems to minimise risks (Moyo, 2019).

In the first quarter of 2019, a risk research-based organisation reported that over 4.1 billion data records were exposed in South Africa (Arewa, 2019). Over 3.2 billion of these breaches were exposed in eight incidents that took place, which means that these incidents are exposing millions of records, and such data is usually in the hands of big organisations and government entities (Arewa, 2019).

The financial sector seems to be the biggest target. In 2019, Equifex, a credit reporting organisation, settled a data breach fine of over R10 million after they were found to have exposed data belonging to 150 million customers (Symanovich, 2017). Ster Kinekor is a cinema chain which has movie theatres in many reputable malls and has also been identified as one of the organisations that had a data breach of over 7 million personal records belonging to customers (Arewa, 2019).

Data security breach fines have the potential to severely cripple a business, impacting on its operations and also damaging its reputation. Therefore, it is prudent for organisations to implement information security measures and to align themselves to comply with the POPIA. Veldron, from a security holding company, has suggested that users should always be on the lookout in the public domain for security violations that affect them (Veldron, 2015). This may be searching for one's personal information on google, checking with the credit bureau for any existing information one is unfamiliar with, and checking one's details with the Department of Home Affairs (Arewa, 2019). This is because certain information can only be made available to the owner later when serious damage has been done. Some people find themselves in the situation of owing retail accounts they are unaware of (Velron, 2016).

The Master deeds data breach is also recorded as one of the biggest data breaches to take place in South Africa (van der Merwe, 2018). This involved a leak of over 60 million data files containing customer information such as directorship positions, ID numbers and address details (Saal, 2018). Intruders are also able to access information such as academic records and credit card information (Saal, 2018; Arewa, 2019). Academic records are usually modified, while credit card information is used to make online purchases and steal the funds belonging to cardholders (Saal, 2018; Arewa, 2019). In the information or data economy, most intruders steal data with the intention of selling it to third-party businesses who use it for marketing purposes. Furthermore, some of the intruders use the data leaked to demand funds from the businesses they infiltrate (Rouse, 2020). As a result, businesses end up paying intruders who have hacked their systems because they fear reputation damage and loss of customer confidence (Rouse, 2020). If an organisation adheres to its local privacy legislation requirements, it reduces its risk of data breaches. While certain breaches might be beyond its level of control, having

adequate measures is key for the business to deter hacking activities into its information resources (Rouse, 2020).

3.13 How does POPIA compare to international standards for information privacy regulations?

The amount of personal data stored by organisations has increased significantly. This can lead to a high risk of data breaches and other illegal activities. Therefore, individual countries needed to come up with ways to protect their citizens' data, resulting in data privacy laws. These laws guarantee the right of citizens and any other affected stakeholders to have their data protected against illegal collection, dissemination, collection, and use. The landscape of the world's data privacy has evolved in response to this. Data legislation differs from country-to-country. Some countries have an active data legislation act. South Africa is still waiting for the president to fully implement the POPIA. The POPIA was developed from GDPR, which is the data privacy legislation in Europe. POPIA compliance does not come close to GDPR compliance. However, tighter alignment with GDPR results in POPIA compliance. Therefore, countries that are GDPR-compliant are close to full POPIA compliance.

The table shows the difference between GDPR and the POPIA (Rocket, 2018).

PoPI vs. GDPR Coparative table		PoPI	GDPR
PoPi Conditions / Minimum Thresholds	Accountability		x
	Processing limitation	x	x
	Purpose specification	x	x
	Further processing limitation	x	x
	Information quality	x	x
	Openness	x	x
	Security safeguards	x	x
	Data subject participation	x	x
Other Areas	DPO* Required	x	x
	Breach Notification	x	x
	Cross border data transfer limitations	x	x
	Electronic Marketing	x	x
	Online Privacy		x

The table, above, shows that GDPR and POPIA components overlap in almost all areas (Botha & Grobler, 2017). The major difference between POPIA and GDPR, which is not described in the table above, is that GDPR is applicable to all EU citizens, regardless of jurisdiction or country where the

citizen is based; while POPIA is limited to data processed within South Africa's borders, regardless of citizenship (Rocket, 2018). If an organisation fails to comply with the GDPR legislation they will be liable for 4% of the organisation's global turnover, or a 20 million Euro fine; and POPIA fines are limited to R10 million (Rocket, 2018). POPIA also imposes imprisonment on non-compliant organisations (Botha & Grobler, 2017). POPIA and GDPR data privacy legislation require companies to have data protection partitioning officers. However, GDPR data practitioners are only required according to the size of the company, the type of operation and the processing ability (Botha & Grobler, 2017), while the POPIA requires all the businesses and entities to have a data partitioning officer in place. Breach notifications are mandatory in POPIA and GDPR, but they are based on timing: GDPR requires breach notifications to be made within 72 hours, while POPIA does not specify a time frame, but requires the organisation to do so within a reasonable period after detecting the breach (Jefferson & Stephens, 2019).

Data Privacy Acts around the world (Botha and Grobler, 2017)

Country	Act	PoPI Principles								Other Areas					
		Accountability	Processing Limitation	Purpose Specification	Further Processing Limitation	Information Quality	Openness	Security Safeguards	Data Subject Participation	DPO Required	Breach Notification	Cross-border Data Transfer Limitations	Electronic Marketing	Online Privacy	Enacted Year
South Africa	PoPI	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		2013
Australia	PA		✓	✓		✓	✓	✓	✓	✓		✓			1988
Canada	PA / PIPEDA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	2000
Europe	EU DPD		✓	✓	✓	✓	✓	✓	✓	✓		✓			1995
Europe	GDPR	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	2016
UK	DPA		✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	2000
USA	*		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	*

The above table shows the international data privacy legislation in relation to the eight pillars of the POPIA. The table shows that the POPIA components are covered in most countries around the world. This benefits cross-border data transfer: POPIA states that countries who are in close alignment with the eight conditions of the POPIA can trade securely (Botha & Grobler, 2017). This means that countries who are not aligned with the POPIA requirements must align to the POPIA. The same applies to South Africa when seeking to trade with European or UK-based entities (Botha & Grobler, 2017). Lastly it is noticeable that the POPIA and GDPR are recent privacy legislation, whilst the others are considerably older. The table further shows that POPIA data legislation components are largely considered, and covered, by most international countries. PIPEDA, POIPA and GDPR make a provision

for accountability. All these laws require a data partitioning officer to be appointed, although they have different requirements on how they are appointed. Because the POPIA is yet to be implemented, certain components might be subject to review before it is enacted (Botha & Grobler, 2017). Therefore, some changes may occur, and certain principles could be changed, or more added.

Before the EU introduced GDPR, they had not had data breach notification in their previous legislation (EU DPD) (Botha & Grobler, 2017). This means that the UK does not have data breach notifications in the DPA legislation. The United States made it mandatory to have notifications (Botha & Grobler, 2017). Data privacy legislation is generally revised. This was the case with the Australian PA, which was updated in 2014 (Botha & Grobler, 2017).

3.14 POPIA implementation challenges in SA, according to the information regulator

The information regulator (IR) has written letters to the president of the Republic of South Africa, requesting that the POPIA legislation be put into effect, and that any missing or additional revisions must be made so that the regulation is implemented within the 2020 financial year (Alkalay, 2020). Moreover, the IR requested the president of South Africa to increase the budget for running the office which to administer the POPIA in SA (Alkalay, 2020).

Advocate Pansy Tlakula stated that the IR needs to be fully funded and with a fully-fledged team to tackle the data privacy issues (Abel, 2020). This is because the POPIA implementation requires more resources to be operational.

The IR has been receiving POPIA complaints from various bodies and seeks to address them (Abel, 2020). Addressing any POPIA-related query requires the information regulator to take certain steps, such as an investigation (Moyo, 2020). While POPIA is not fully implemented, it is important for businesses of all sizes and budgets to find ways to be compliant with the POPIA, as it would be very expensive for them to fast-track their compliance process when the POPIA is in effect (Moyo, 2020). This means that businesses must have a certain level of POPIA compliance within a specific time frame. Instead of having to implement the POPIA plan rapidly, entities should nurture an existing compliance system, which would result in an inexpensive, rapid compliance plan (Moyo, 2020). The IR will give all the private and public bodies a period not exceeding a year (12 months) to be fully compliant with the POPIA (Xperien, 2020). The eight POPIA components are complex and may require more than 12 months to implement (Xperien, 2020).

The chairperson in the IR's office said in an interview that they had made certain key applications in the IR's office (Mzekandaba, 2019). In addition to this, they said that South Africa's data privacy legislation implementation is falling behind, while technological advancements are growing at a rapid

rate (Mzekandaba, 2019). The use of systems in the government and private sector continues and private individuals' data are collected (Xperien, 2020).

There are various data processing systems such as the SARS e-filing system; the banking system; the traffic fine system; the government social grant application system; payment systems; online learning systems; and e-commerce systems used by data subjects through the use of the internet (Xperien, 2020). These technology solutions, advances and deployments in the country have increased the urgent need for data privacy legislation to be in place (Xperien, 2020). Everybody who interacts with the aforementioned technology systems have private and public lives, and each individual must be given the autonomy to decide what can be made public or stay private, and to choose how their data is used when collected (Mzekandaba, 2019).Therefore, data privacy matters and is a human right (Right2Know, 2016). While it may seem that data can be processed into information, and as such would enable businesses to promote their products and services, thereby increasing the GDP, personal data can be used by criminals in severe, life-threatening matters (Reuters, 2018). Cybercriminals use entities' data to harm them (Reuters, 2018). Identity thieves who steal people's identity or clone bank credit cards are some of the results of data privacy violations (Jougleux, 2012). This increases the need for the IR to be fully operational and running the POPIA. Without the implementation of a fully functional IR, South Africans will be left with entities who will collect their private information, exploit and abuse it, and still not face any legal repercussions; in short, criminals will be left to exploit South African's personal information (Donnelly et al., 2018). In a data-driven age, the government should have a measure in place to forecast how the POPIA will be implemented (Jougleux, 2012).

The IR stated that, among the numerous data privacy breaches and case complaints received from the public, many are about marketing companies who send unsolicited chain marketing SMSs directly to consumers These complaints were reported to the IR office through social media or email (Donnelly et al., 2018; Fynn, 2018). As a result, they have started putting surveillance on the SMS distributors. According to Burger-Shmid, the IR has done a remarkable job in investigating complaints received from the public via social media, even when they have limited resources (Burns & Burger-Smidt, no date). Furthermore, Burger-Shmid added that the IR has increased the organisation's visibility on social media and is following-up on reported data privacy matters (Burns & Burger-Smidt, no date).

One of the key tasks allocated to the IR is to increase awareness of the POPIA legislation (Michalsons, 2019). Therefore, the IR sent a strong message to the market to inform them that her office is taking POPIA compliance seriously (Crouth, 2020). This means that organisations have been reached, and the businesses that have been found in breach of the POPIA will have a record with the IR. Such records may resurface when future investigations are done, and the IR office is fully operational (Crouth, 2020).

This will consequently put the bodies who are bypassing the POPIA legislation at high risk of law enforcement consequences (Crouth, 2020).

Cowling stated that the Treasury Department in South Africa must prioritise digital security (Crouth, 2020). This is because the data privacy matters which are linked to cybersecurity are currently in the hands of those in the legal fraternity, which is not entirely the correct space, because cybersecurity measures require technical experts who have the capacity to deal with such matters (Crouth, 2020). The cybercrime bill in SA has been substantially changed and more pressure has been put on the police officers to investigate such matters. This puts the police officers under more pressure as they are dealing with more criminal cases (Crouth, 2020). Therefore, the implementation of the POPIA will make it easier for the IR to deal with enforcing compliance.

Pinnok, a cybersecurity expert, has sited the delay in the implementation of POPI as creating market uncertainty (Crouth, 2020). The legislation has been there since 2013 and it has been delayed. Furthermore, Pinnok said that organisations have waited since 2013 for legislation which has not been implemented (Crouth, 2020). This may give the market a reason, justifiably, to not invest in technical measures for achieving compliance because they may not realise the return on investment (Crouth, 2020). It may take many years to build a data privacy legislation programme (Crouth, 2020).

3.15 Issues faced by businesses in implementing the POPIA.

These are challenges of implementing a POPIA in the SME and other businesses sectors.
This is because privacy legislation impacts how businesses operate and imposes restrictions on daily business activities (MPREM, 2017). In the e-commerce sector, this could mean that customer data are handled with strict privacy rules and customer-centric permissions (MPREM, 2017). Businesses are yet to be given 12 months to be POPIA compliant, and some have already started working towards aligning to the POPIA (Right2Know, 2018) However, they encounter challenges which hinder their implementation plans.

3.16 Understanding condition 7 of the POPIA

POPIA is a legal document which does not provide many details on how the technical implementation should be done (Sikhungo, 2015). The 7th condition of the POPIA, which is ‘Security and Safeguards’, is a technical component which requires technical details informing implementers on how, and what, is required for POPIA compliance (Sikhungo, 2015). According to the POPIA 7th condition, businesses are advised to seek best practices for implementing the security safeguards (InfoReg, 2013). Whilst industry best practices are available, they are costly, and businesses still find it difficult to implement a POPIA without a comprehensive guide, and advice on which specific best practices to consider

(Sikhungo, 2015). As a result, businesses have been left with a challenge of planning for compliance. A bigger challenge posed by the 7th condition is that there is no implementation framework available for businesses to adopt for implementing the technical requirements of the POPIA (Sikhungo, 2015). Lastly, there are several best practices which can be used jointly by organisations to adopt the requirements of the condition 7. These are, but are not limited to, COBIT 5, ISO 27001, ISO 27002, KING 3 (Goosen & Rudman, 2013). Some organisations may find a way to meet the requirements of condition 7 of the POPIA by creating their own custom methodology (Sikhungo, 2015). This can be done by the technical team who can find applicable measures which are available, and use them to create a single, customised POPIA framework (POPIA (Pty) Ltd, 2015).

Implementing a comprehensive information security management system is cost-heavy (Sikhungo, 2015). However, entities need to secure their computing assets (Kandeh, 2018). In addition to this, organisations must allocate and dissect a budget for satisfying the requirements stated in the POPIA (Kandeh, 2018). This means that technical staff need to be employed; security software must be purchased; IT hardware for securing data must be implemented; company IT security policies must be updated; industry best practices and standards must be adopted; and the whole organisation must be trained and be prepared for implementing the requirements stated in the POPIA (Kandeh, 2018). These come at a cost which is budgeted by the organisation. As a result, implementing the POPIA is not a low-cost practice.

One of the fundamental areas of POPIA compliance is consent from data subjects. As mentioned, data subjects refer to the individuals who own the data. In the e-commerce scenario it can refer to a customer, employee or any other stakeholder who owns the data being collected from the e-commerce application (PwC, 2011). Furthermore, it is prudent that a data subject consents to their data being collected and stored in a public or private organisation's database. The consent can be given through a terms and conditions section added into the site, where the data subject agrees to sharing their data (PwC, 2011). The consent must be explicitly stated. This includes what the data collecting party aims to do with the data. Organisations find the process of obtaining consent from the data subjects a challenge. Most data subjects refrain from allowing organisations access to their personal data (Sikhungo, 2015). This task brings a huge administrative burden to the organisation to ensure that they do not exceed the boundaries of the POPIA when collecting data subject information (PwC, 2011).

Businesses trading in different continents and countries should trade when privacy legislation permits them (PwC, 2011). This trade is conducted in virtual space and results in customers receiving goods or services from foreign countries. A good example would be the famous alibaba.com and wish.com multivendor online platforms, where the international community purchases products offshore. These online vendors must meet the minimum POPIA requirements before South African subject data is

transmitted out of South Africa (PwC, 2011). This promotes data privacy because offshore organisations would meet the data privacy legislation of South Africa. If the country where the South African data subject is purchasing online goods or services is not POPIA compliant, then they are in breach of the POPIA (Michalsons, 2020). Moreover, it is important that there is a compliance monitoring process which will be used to measure the success of an organisation's POPIA implementation efforts (Michalsons, 2020). In the e-commerce scenario, this would mean that an organisation would have a checklist stating the security measures on the internet site, and checking if they are functional, for example, if a site has the HTTPS and the digital security certificate is working (ITWeb & Weidemann, 2018).

3.17 Information security management systems as a tool for POPIA

ISMS is short for 'information security management systems', and refers to a system and controls, processes and policies which organisations adopt for businesses to manage their sensitive information and ensure that it is secured (Dutton, 2019). ISMS can be used to flatten the curve of security-related vulnerabilities, which are always on the rise. These processes in the ISMS allow organisations to develop an information security plan for maintaining integrity, confidentiality, and availability of their information resources (Dutton, 2019). This may be an online store, planning how they would implement an information security system, looking at all the elements in the ISMS, and implementing them. These measures can be technical, managerial, and financial. Therefore, they affect every level of the business.

ISMS encompasses processes which include people, risk management, and IT processes to protect businesses activities from interruption. ISMS aids SMEs, or any-sized organisation, in securing their information assets, which are critical to their operation. The ISMS risk assessment component requires an organisation's personnel to assess the organisation's security risks and to define them (Dutton, 2019). The defined outcome may require additional ISMS controls to be activated. These controls are put in place to guarantee business continuity when the risk is experienced, and may be a backup procedure when the database storing customer records is compromised (Shedden, 2010). The backup-and-restore procedure enables organisations to resume operations.

Image source (Anita, 2017)

3.18 How ISMS can assist SMEs with complying with the POPIA.

Information security procedures and policies are prescriptions set by an SME's IT security unit, for implementing an IT infrastructure, data, and network (Anita, 2017). The whole business must adopt the prescription and its boundaries. This means that the business will have IT security rules, such as that all computers must be password-protected, and can only connect to external Wi-Fi when connected to a VPN (Anita, 2017). Therefore, all computers handed out by the IT department will be password protected and have VPN software installed. These policies extend through all levels of IT implementation, affecting all the computing resources that affect business continuity.

An information security asset refers to any asset of value to the business and information services (Anita, 2017). This can be a database which contains customer data. Physical assets can be the servers and hardware equipment, and the people who operate the information assets (Anita, 2017). Asset management in relation to the POPIA describes a situation where an ISMS is adopted to protect assets that affect business continuity and align them with policies, so that they are used in a way that poses less risk to the organisation.

Physical and environmental security are processes for protecting business buildings and infrastructure against threats (Anita, 2017). This can be enforced by employing a security guard, enforcing fingerprint access to the building, and locking physical information assets away. In the event that physical security is affected, a contingency plan will be adopted (Shedden, 2010). The plan will enable business continuity and protect the business's information.

Employees, and any contractor, who access sensitive information in an organisation, must understand their roles and limitations on the data they are accessing. This involves not sharing information with people who are not authorised (Shedden, 2010). The organisation must also revoke data access for employees who are no longer working for the organisation.

A physical security component comprises regulations that govern who can access a building or room containing a sensitive information resource (Shedden, 2010). These are keys that unlock the server room, or fingerprint access given to individuals who must access a room or building, or passwords that are used to authenticate users who access a computing network in an organisation (Anita, 2017). These passwords are used to allow authorised users access to the network. Certain employees may view more or less information based on what they are employed to do, so the HR department has access to payroll information, the sales department has access to customer records; but the secretary would not be given such access (Anita, 2017). Therefore, an organisation that runs an e-commerce business must ensure that they have adequate access control measures in place, because sensitive customer information such as names, surnames, delivery addresses, and buying patterns are stored in a database and are prone to abuse. Organisations, in general, give employees a non-disclosure document to sign. This is a legal document that specifies that the employees should not disclose the contents of the data they access to anyone who is not within the boundaries specified by the organisation.

Incident management refers to measures taken by an organisation to analyse and deal with incidents, or hazards that can take place unexpectedly (Anita, 2017). Therefore, incident management in IT security may refer to a security breach or a hack that has taken place. This could mean restoring a database; such tasks are generally handled by an incident response team. An organisation once had its customers' credit card information hacked, and they had to report the incident to the customers, so that they could block their cards and avoid illegal use of the cards (Anita, 2017). This incident was then managed by a cybersecurity team by guaranteeing their card detail security (Shedden, 2010). The organisation was then able to continue operating.

This process enables an organisation to restore their services when they have experienced an incident/disaster (Shedden, 2010). This means an online store will resume its operations and be able to serve its customers. In an e-commerce business, this involves testing the website to check if it is operating as desired. Business continuity is vital for any business to continue operating after experiencing an incident. Most new businesses manage to continue with operations if they have a comprehensive ISMS because incidents are anticipated and risks are identified (Shedden, 2010). Some risks that face businesses are not common and might not be reflected in their list of identified risks

(Anita, 2017). However, such risks might delay a business's continuity plan schedule. Such challenges give organisations opportunities to re-evaluate their risks and plan for unforeseen risks, thereby enhancing their business continuity plans.

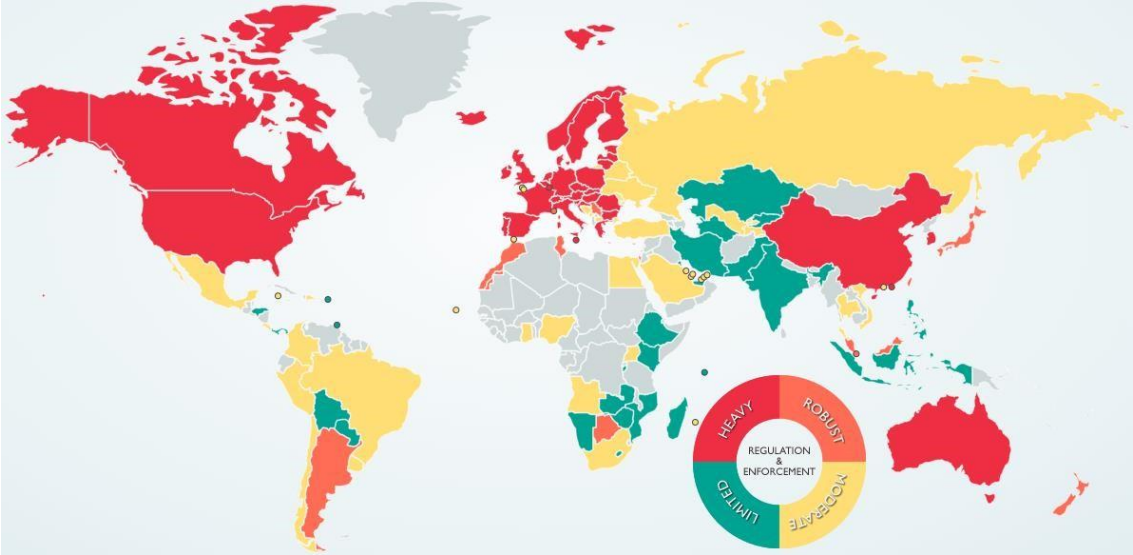
Organisations must have a compliance management process in place (Anita, 2017). This process is practical in e-commerce, where they adopt a secure buying environment in the payment system, where customer data is protected. All online stores must have terms and conditions and privacy policies (Anita, 2017). These are the rules that need to be adhered to before the site can be deployed for customers. Therefore, the managers in the business must ensure that they are compliant. This is the component that enables businesses to align to laws such as the POPIA.

POPIA regulations are concerned with how a business is going to store data, and the security measures put in place to ensure that the data is protected from intruders who seek to violate it (Kraft & Kakar, 2009). Furthermore, customers who shop on e-commerce sites usually have trust in the platform that they are giving personal information to. Therefore, it may be detrimental for an online business if it loses a trustworthy customer, as this may give the business a bad image, causing it to lose more customers and go out of business (Kandeh, 2018).

Compliance management requires that the employees in a business, who are tasked with the process of ensuring security, tick all the compliance regulation boxes (Kandeh, 2018; Michalsons, 2019).
Compliance is not a once-off activity – it requires constant updating as rules and regulations are updated. Compliance management may also require an organisation to have a large budget, as certain regulatory requirements may result in updating the entire security process of an e-commerce site, such as changing the structure of the database and updating data encryption standards. Failure to comply makes the business liable for large financial fines and may also lead to prosecution (InfoReg, 2013).

ISMS processes can be tailored according to the business's needs and size (Dutton, 2019). Larger ecommerce businesses, such as Takealot and Alibaba, have enough financial resources to afford a complex ISMS plan for incident management. However, SMEs (that are usually start-ups) have fewer financial resources and cannot afford an extensive information security management system. Therefore, they can adapt an existing, affordable ISMS which allows them to comply.

There are consulting organisations that provide ISMS consultation services (Dutton, 2019). These organisations are specialists in this area. With the assistance of such organisations, SMEs are able to purchase ISMS packages to which they can adapt their business processes, and so be able to respond to incidents. Lastly, ISMS enables a certain level of compliance with data privacy legislation and can aid, to a certain extent, in keeping the organisation's information asset secure (InfoReg, 2013; Dutton, 2019).



Current global data privacy legislation and enforcement (Piper, 2020)

The above map of the world indicates data privacy legislation levels, by country. It shows that most countries in the world have some form of data privacy laws and they enforce them. Countries which are indicated by red on the map have strict data privacy legislation. Countries coloured in amber have moderate, and the ones in green have limited, data privacy legislation. The countries which are not coloured (in grey) have no data laws and legislation in place. They do not enforce any data regulations, and they also stand a risk of not trading with countries which have heavy-to-moderate data privacy regulations and enforcement.

GDPR (General Data Privacy Legislation) is European-based data privacy legislation. The United Kingdom was a full member state of the European Union when GDPR was passed in May 2018.
However, due to political differences between the United Kingdom (UK) and the European Union, the UK left the European Union. The treaty signed by the UK and European Union required that the UK enforce the GDPR legislation until the end of 2020. However, given the importance of data privacy, the UK government has developed its own data privacy legislation named the Data Protection Act 2018 (DPA) which worked alongside GDPR until the end of 2020.

The People's Republic of China (PRC) does not have comprehensive data protection legislation. However, laws that relate to the protection of personal information are merged into a complex framework, and form part of various laws within China's regulations. A part of this law is called the Tort Liability Law and the General Principle of Civil Law. These laws have been used to cover the data protection rights of citizens. The challenge with these laws is that they are not explicit. Therefore, they are not easy to interpret and implement.

The PRC needed to put an explicit and comprehensive data protection law into place. In response to this, they developed a cybersecurity law which came into effect on 1 June 2017. This was the PRC's first data security and privacy law. Since then, they have added multiple guidelines on how such rules and regulations can be adopted. The PRC trades vast quantities globally. Online marketplaces such as Alibaba originate from China, and have been trading internationally. The PRC took a decision to protect information that flows online in December 2012 and in February 2013 enacted a law that governs online information systems.

The Australian government regulates data privacy through a mix of state laws. The (FPP) Federal Privacy Act of 1988 is an Australian-based privacy act which is only applicable to the private sector with an annual turnover of a minimum of AU$3 million. This includes all the government agencies and commonwealth governments in Australia.

Most of the territorial states in Australia (excluding South Australia and Western Australia) are regulated by their own information protection legislation, and these are applicable to state agencies that directly work with government agencies. The laws include:

Data privacy laws

Act/ Law	**Year**	**Australian Territory**
Information Privacy Act	2014	Capital
Information Act	2002	Northern
Privacy & Personal Information Protection Act	1998	New South Wales
Information Privacy Act	2009	Queensland
Privacy and Data Protection Act	2014	Victoria

The Australian territorial laws (above) cover various sectors, including healthcare, online businesses/ecommerce, financial services and telecommunications. These laws are designed to limit how information is processed and to protect the data privacy of individuals living in Australia. The Privacy Act applies to:

- individuals;

- corporate organisations;
- trusts;
- partnerships; and
- unincorporated organisations.

The privacy commissioners in Australia oversee enforcement. They generally investigate breaches and receive reports of privacy information breaches. Depending on the outcome of the investigation, the privacy commissioner may do the following:

1. dismiss the complaint;
2. make recommendations to the party to rectify their act;
3. issue a fine of up to AUS$ 420 000 to individuals; or
4. issue an organisation with a fine of up to AUS$2.1m.

Repeat offenses may result in larger fines and possible imprisonment.

Germany has the obligation to appoint a data protection officer, in response to its data privacy laws. Data protection officers must satisfy the following requirements:

- they must be a public authority;
- they must monitor data subjects on a large scale, as their core activity; and
- their core tasks are to protect sensitive personal information on a large scale.

The data protection officers must be well informed of the data protection laws in Germany. They must ensure that they manage all information security matters, from data privacy to receiving information about security leaks. Below is a short job description for a DPO, according to GDPR guidance, which has been adopted in Germany:

- Inform and ensure compliance with GDPR and other member state data privacy laws.
- Provide advice and monitoring of data privacy impact assessment.
- Monitor compliance with the law and provide training and awareness.
- Be the point of contact on information security breaches and act as a supervisory authority.

Some African countries do not have comprehensive data privacy laws, and do not have any data protection practitioners. However, their data privacy laws are entrenched within their constitutions, where they are not detailed. These counties include Zimbabwe and Angola, to name a few. Seychelles has legislation, but does not have any data practitioners in place. These are some of the countries which have the fewest data privacy laws and generally do not enforce them.

Zambia has enacted the (ECTA) Electronic Communication and Transactions Act. This act includes steps and guidelines for e-commerce businesses and websites. Furthermore, the act governs all online transactions, regardless of whether they are commercial or not. This act works alongside the Consumer Protection Act, which seeks to guard against businesses that abuse consumers rights. Chapter 5 of the ECTA provides a list of customer personal information that can be stored by vendors in their databases or displayed on the websites. South Africa has also adopted the ECTA, to regulate data stored electronically on websites until the POPIA is fully implemented. The ECTA does not require the appointment of a data protection officer. In Zambia, if an entity is found in data breach they can be charged, and if found guilty, fined up to $12712, or sentenced to up to five years imprisonment.

Lesotho has a Data Protection Act. Section 15 of this act requires the appointment of a data controller who is designated to appoint a data officer, who oversees enforcing the data laws of the country. This indicates that Lesotho does not have comprehensive data protection regulations and they do not have strong data privacy enforcement in place.

Botswana's Data Privacy Act has not yet been implemented. However, they have drafted a data law that has what is called a data controller. The role of the data controller is to appoint a data protection practitioner. The role of the data protection representative is to ensure that the Data Privacy Act is adhered to and to attend to all matters concerning data privacy breaches. Furthermore, they should ensure that data privacy laws are enforced through legal routes in the country. Botswana's data privacy laws are not strict, and they are not enforced in most cases. Since the law has not yet been implemented, no fines or possible imprisonment has been prescribed.

Namibia appointed an office which oversees the entire information communication technology sector, including information security. The office is called the MICT, also known as the Ministry for Information Communication Technology. The vision of this ministry is to develop ICT in Namibia. The ministry is also tasked with appointing a telecommunication and information authority who manages the regulations on telecommunication and the transmission of information over the internet. This involves matters relating to data privacy and ensuring that information transmitted over the internet is safeguarded. Furthermore, the ministry will receive notifications on information security breaches. Lastly, any party found in breach of data privacy legislation in Mozambique is not liable to a fine or imprisonment. Mozambique does not have specific data privacy legislation, like Zambia and Botswana. They have other legislation that enforces data privacy:

- the electronic transaction laws; and - the labour laws.

These laws are designed to govern how electronic information is disseminated and used by private and public bodies, thus protecting the privacy of citizens' information. However, these laws are not generally enforced by the government. The disadvantages to countries that do not enforce, or have limited, data privacy legislation, are severe because they may be denied the right to trade with countries that enforce data privacy legislation. The lack of legislation may limit transactions with such countries and could make it difficult for the counties with limited data privacy laws to conduct business externally, especially with countries with major currencies. The Mozambican authority may sentence any entity in breach of data privacy to three years of imprisonment, of which one year may be paid as a fine. These enforcement rules depend on the level of the data breach. If the data breach was the result of fraudulent activities, then the penalties are higher.

In 2017, the judges that head the constitutional court of India started a petition that stated that data privacy is a constitutional right. This led to the drafting of a data legislation bill in 2019. Previously, since 2000, India had had an Information Technology Bill. This bill covered electronic data privacy, and governed how public and private bodies could use and process data belonging to entities. This IT bill was passed in 2011, and is still currently implemented in India, through the IT Ministry. The Information Privacy Bill of India covers extensive data privacy issues, including cross-border data transfers, and how data flows from end-to-end. Given that India is one of the leading IT capitals in the world, they need to have their data privacy policy and enforcement in place.

Mexico has adopted the Federal Law of Information and Data Privacy for data processed and stored by private organisations. This law was enforced on 6 July 2010. Other privacy laws they passed include:

- privacy notice guidelines, in April 2013; and
- recommendations on data security, in November 2013

The laws apply to personal data when:

- the data controller processing the data is in Mexican territory; but
- if the data is processed for a Mexican data controller, this can be anywhere in the world; and
- when the data controller is using means located in Mexican territory to process the data, but processes data for a different territory.

The Mexican data privacy regulations are applicable to private bodies, but not to government. Enforcement in Mexico may lead to a fine of M$8836, or even between three months and six years imprisonment.

The United States of America has several specific data privacy laws which regulate different sectors, such as:

- healthcare;
- financial services;
- credit information;
- children's information;
- telemarketing; and
- telecommunication companies.

The USA has hundreds of data and privacy security measures within its 50 states or territories. These are requirements imposed to ensure how data is processed and disposed of, they ensure the protection of social security numbers, and cover breaches and the notification of breaches. California itself has over 25 state data privacy laws, including its recently enacted (CPA) Consumer Privacy Act which was put into effect as of January 2020. The CPA covers specific data transmission laws that look at how information is collected, why it is collected, restrictions on the data, and why the data could be disclosed. Several US states are currently lobbying for state-level data protection and privacy legislation which covers the entire USA. The legislation should be like the Californian's' CPA, in general, but may include further conditions and other requirements.

Moreover, the USA's FTC (Federal Trade Commission) has jurisdiction over various commercial organisations to protect consumers against deceptive or unfair business practices. Furthermore, the FTC has powers to enforce certain laws on privacy and to investigate companies for the following:

- not implementing reasonable data and privacy security measures;
- violating the privacy of consumers, which involves how to use and store their data;
- sharing consumer information with entities which were not disclosed to the consumers and - modifying consumer information and misrepresenting them to other entities.

The USA does not indicate the amount of money payable by fines. However, they have stated that there will be heavy financial charges linked to such security breaches.

Kenya has the Data Protection Act which came into effect in 2019. The act prohibits organisations or individuals from sharing people's data regarding:

- ethnic group;
- health status;

- financial information;
- genetic data;
- origin;
- gender;
- spouse; and - children.

Data controllers are obligated to report any breaches to the DPC within 72 hours of becoming aware of the breach. Data practitioners must inform data controllers of the breaches within 48 hours after being notified. The act was adopted in November of 2019, and it is the main law that regulates data privacy in Kenya. Moreover, this also applies to online transactions that take place over the internet or ecommerce sites. Kenya employs a data protection commissioner who oversees the implementation of the regulation and ensures that they have a data practitioner who assists in managing the unit to implement the regulation. The data officers are also tasked with the following:

- ensuring that the act is adhered to;
- making sure that stakeholders have capacity and knowledge of the act; and - provision guidance on data protection impact assessment.

The DPC in Kenya oversees the investigation of data breaches and imposes fines on parties who violate the data privacy legislation. The fines can be any amount up to 30 000 Kenyan shillings.

Canada's legislative body has passed 28 federal territorial and provincial privacy laws. The privacy requirements in these regulations cover the following:

- anti-spam: distributing repeated chain messages to individuals;
- identity theft / criminal code: pretending to be someone who you are not, using legitimate information belonging to someone else; and
- protecting health data in the public and private sectors.

Each law is different in scope, remedies, enforcement, and substantiate requirements. Canada has a comprehensive law for the collection and dissemination of personal information. The summary, below, describes some of the privacy and information-processing laws:

- PIPEDA: Personal Information Protection and Electronic Documents Act.
- PIPA: Personal Information Protection Act; and
- PIPITA: Personal Information Protection and Identity theft Prevention Act

PIPEDA is applicable to employers and employees of telecommunication and healthcare organisations, and organisations which sell information belonging to entities without their consent. It is enforced by privacy regulations and decisions on making findings and recommendations. A court may be given instructions to review the findings. The penalties may lead to a fine or possible imprisonment. However, if the actions were an attempt to sell information illegally, there would be heavy fines.

The South African government has data privacy legislation. However, over-and-above it, comes the Bill of Rights, included in the Constitution of South Africa, which specifies that data privacy is a human right, but only to a certain degree. Therefore, data privacy is a human right in South Africa, but there are limitations to it. The South African data privacy legislation is the POPIA (Protection of Personal Information). This piece of legislation has been developed as a directive on how data privacy should be applied. Enforcement may involve heavy fines or even possible imprisonment. Those found in breach of this act, and acting without following the appropriate measures as indicated in the act, will be prosecuted. If the breach occurs in a company, that company will be required to pay the fines; if it is an individual, the individual will be liable for the fine.

Business growth in Africa is paramount, and organisations in Africa need to have measures in place to implement IT security legislation and make international trade possible. Not all countries in Africa are governed by data privacy legislation. There are 17 African countries that have legislation on data security. These countries include Angola, Lesotho, Morocco, Tunisia, and Ghana, to name a few (Signé & Signé, 2018). These countries have adopted comprehensive data security legislation and have data breach notification plans in place. The African Union planned an information Security / Cyber Security Convention in 2014, with the intention of developing a continental data privacy law. However, it was not adopted. Therefore, the issue of data security is the responsibility of each African nation through its own data security policy.

The POPIA is not yet fully implemented within South Africa, but some organisations have adopted certain parts of this act. The 7th condition of the POPIA requires technical implementation, yet the POPIA itself does not provide any directives on how businesses can meet the requirements of the 7th condition.

3.19 Current state of POPIA compliance in the e-commerce sector

The e-commerce sector's POPIA maturity levels are measurable, but most stakeholders in the sector do not divulge their legislation compliance levels because they fear being audited and being taken out of business (PayU, 2017). Therefore, this suggests that the compliance levels in e-commerce are not mature, but that they do have knowledge about the repercussions of POPIA non-compliance (PayU, 2017). It is important for research to be undertaken in the POPIA space because some organisations are

seeking to be compliant but may have little or no knowledge of the required measures that need to be taken for them to be compliant.

POPIA compliance can be measured from the 7th condition (Michalsons, 2020). These are the technical components which are not detailed in the POPIA, but explain to businesses the relevant existing standards, best practices, and regulations (PwC, 2011). Data privacy legislation are often neglected, especially when not enforced (Michalsons, 2020); yet data breaches can lead to reputational and financial damage for any business (Pillay, 2014).

The table, below, outlines the general technical requirements for data security in e-commerce (adapted from Pillay, 2014)

Item	Description
Encryption	Encryption involves scrambling text into an unreadable form. This type of text is then later decrypted to make it readable by a validated user. This level of security is used when data is transferred between two computing endpoints which communicate via an internet connection. The data is protected in transit and at the destination, as well. The destination is usually a database repository. There are many encryption standards which work, based on complexity.
Secured data repository	A data repository is a location where data is stored. Data repository protection software is used to protect and block intruders from accessing the repository without permission. This requires the authentication of users before they can access the data source. Therefore, ecommerce data repositories are generally protected.

Backup and restore	A database which is stored and contains data must be backed-up in case it is affected. The backup copies are kept so that an organisation has reliable data in case of a database disaster. Most ecommerce businesses do this for business continuity, and this security component is sold by third party organisations.
Password policy	A password policy is enforced by an algorithm on the system, and users choose passwords with mixed patterns. These patterns are special characters, numbers, and uppercase and lowercase (%$!*(@&^PAGT), instead of using
	simple passwords such as ID numbers or last names. Such patterns are used to make a password complex. Therefore, it makes it difficult to guess and thereby offers protection. Such an algorithm is adopted by the businesses that own the site.
Secure site (SSL certificate)	SSL certificates are used to digitally sign a website and place a padlock next to the site's URL. This gives confidence to the users that the site is valid and reliable, and that the information is secured when the user is browsing on the site.

Not storing banking details	E-commerce sites reduce the risks of storing customer banking details by borrowing methods from modern application programming interfaces (API) where the buyers are redirected into a safe banking site owned by a merchant, and this is where the payments for goods and services are made. As a result, the banking details belonging to the bank are not stored on the e-commerce site's database. This reduces the level of vulnerability of the database because users' banking details are not kept in the database.

The information in this table informs us of the levels of compliance for e-commerce businesses. Whilst the POPIA demands that more be done, these minimum measures taken by online businesses can be tightened and aligned to the POPIA requirements for full compliance.

3.20 Taking compliance and E-commerce and putting them together.

Compliance means conforming to a regulation, a law, or a rule (ICA, 2018). Regulatory compliance in e-commerce means that the e-commerce businesses strive to be aware of the law and take the necessary steps and measures to proactively practise what the laws and regulations require (ICA, 2018). A compliant business is known to have satisfied all the requirements and may even be awarded a certificate of compliance. When an e-commerce site has a valid SSL certificate it signifies that they have a certain level of security on their sites, and that the padlock contains the certificate and its details (Guides, 2019).

3.21 Benefits of compliance with the regulations for business, adapted from Davidovic (2014)

A) It reduces risks that can affect the business.

   An e-commerce business that is compliant reduces the risks associated with fines and violating the rules. Therefore, the money not paid for fines can be used to increase business efficiency and capacity. This may mean that the funds that would have been used to pay for fines can be diverted into more research and satisfying customer needs. Furthermore, regulatory breaches attract media attention, which could lose the business customer confidence.

B) It helps realise the business's mission.

Most e-commerce businesses have a mission, vision, and values to protect customers as part of their corporate responsibility. Therefore, a business would be irresponsible if it is inconsistent in following its values and business mission. When laws and regulations are properly drawn up, they not only address external laws, but also company aspirations. Therefore, businesses should have internal and external aspirations to be compliant. Failing to do so means that the organisation has failed to do the right thing in upholding its business mission.

C) It generates confidence and results in less internal hesitance.

An organisation that does not follow the required rules and regulations is tantamount to a road intersection that does not have street signs, and traffic lights. Such roads are generally unsafe and are prone to road fatalities because they do not have rules. On the business side of things, lack of adherence to regulations threatens the confidence of staff members because they generally do not know what to do next, or what action to take while completing tasks. Therefore, it is important for organisations to follow regulations so that they inspire confidence in the workforce. A business that follows such regulations can prevent paralysis and improve business success. The employees can address clients with confidence when dealing with their data and ordinary job protocols.

D) It leads to better a relationship with stakeholders and regulatory bodies.

When stakeholders and regulators deal with businesses which are ethical and known to uphold regulations, it improves the business's operations because they can ask for advice, which enables richer discussions; and the business can act with a high level of confidence because the advice is given from the regulatory body, directly. Regulators in general view companies that follow standards in a different light. However, these companies do not get any privileges or favours.

E) It improves business transparency.

Businesses in the e-commerce sector rely heavily on reputation capital. In POPIA compliance, a customer may require transparency regarding their records. If an organisation keeps such information from the customer, they have ultimately disobeyed the 'openness' pillar of the POPIA. It is prudent for the business to be transparent and honest with the customer to gain customer confidence.

F) It helps to attract customers and grow the business.

When e-commerce businesses adhere to rules and regulations, they are generally successful because they are focused on driving business success. Therefore, customers are able to draw attention to compliant e-commerce stores and would prefer to buy and sell through them. The biggest marketing tool is word of mouth: it comes as a testimony and attracts more customers. Following regulations helps business growth. When a customer knows that their records are privately kept in a specific e-commerce business database, and it does not violate their data privacy, they tend to speak well of the business, thus promoting it to more potential customers. More customers mean more business and growth.

G) It helps provide details to make better decisions.

E-commerce businesses, just like any other businesses, have a top-down method of operating. The bottom-level operations are run by the front-liners who are responsible for developing, marketing, and supporting the site (Data Privacy Manager (2020). These are the individuals who would put in all details and report back to management about the efficiency, or issues, at the bottom level, where the business interactions take place. This level is where all the documentation is drawn up, and management can improve areas that need it, whether it be errors in the database, or hacks, or how the marketing team gets consent to promote the business. As a result, the business can get better data and information to utilise investments wiser. All this is a benefit of compliance.

3.22 Data privacy for consumers

Consumers have the responsibility of protecting their data privacy. In addition to this, it is vital that they do not expose their passwords, and other data privacy information. In the event a consumer exposes their information, intruders may have access to it (Data Privacy Manager (2020). There are various ways in which a consumer leaks their own privacy information, including leaving their computer unlocked and unattended, or sharing their passwords with strangers over the phone/email. When the data is leaked, the intruders can access sensitive information and conduct transactions which should only be conducted by the legitimate person (Data Privacy Manager (2020). Therefore, the owner of the information has the responsibility of protecting their data. Below are some of the approaches that can be adopted:

- multiple factor authentication;
- updating security features of devices;
- being cautious of odd requests;

- creating regular data backups;
- passwords-protecting devices; and
- not sharing sensitive information such as passwords.

3.23 Multiple factor authentication

This enables the owner of the information or accounts accessed to reauthenticate any service request made against their accounts. Therefore, if the request is made fraudulently, the owner of the data would block the request (Data Privacy Manager (2020). For example, a user would need to use a cell phone application to authenticate a website attempting to access their banking profile.

3.24 Updating security features of devices

Computing devices have security patches that are released by the software vendor this includes companies that own software applications. The software applications must be updated so that the users have an updated version, which in most cases have key security upgrades.

3.25 Being cautious of odd requests.

There are individuals who work hard using fake website links and other browser sniffing methods to steal user data. The owner of the data must be cautious of such sites, links, and text messages.

3.26 Creating regular data backups

A data backup is a data repository which replicates and updates an existing live data repository, with the aim of being accessible in the event a user is affected and unable to access their live data (Data Privacy Manager (2020). The backup ensures integrity and authenticity of the original live data when the live repository backup is affected.

These are some of the approaches that may be adopted by data owners to safeguard their own information assets (Data Privacy Manager (2020). Not all incidents are a result of a data hack; some are a result of users leaving their computing devices unattended or sharing their secret information, such as passwords, with people who work hard to gain illegal access to the data.

There is no legislation that limits how users use their secret information (username and passwords). However, organisations always provide users with awareness information to ensure that they are knowledgeable about keeping their secret information safe from intruders. This is because organisations are generally blamed when a user's data is accessed by an intruder. However, it is difficult for any organisation to determine how intruders have gained access to an information asset belonging to a customer. Therefore, customers must play a role in ensuring that their data is protected from their side.

3.27 Data privacy

The terms ‘information privacy’ and ‘data privacy’ may be used interchangeably, but refer to the same domain, which is part of data protection. These terms pertain to proper data handling through data privacy legislation. Data privacy is about how data should be managed; stored; shared; collected from the primary; third parties; and the applicable state data privacy organisations. Some of the data privacy regulations, as mentioned earlier, are CCPA, POPIA and GDPR (Data Privacy Manager (2020).

Data protection wings: security and privacy. The security wing includes encryption; network security; activity monitoring; access control; and breach response. The privacy wing contains the consent; policies; data removal; management of third parties; discovery; and classification. The data security wing indicates how the data privacy policies are enforced, while the data privacy wing indicates why, and what, data is important. The aim of both wings is to ensure that usable data is protected.

3.28 Components of data privacy

There are three elements that make up data privacy. These elements are (Data Privacy Manager (2020):

- an individual having the rights to have control of their personal data;
- practices and procedures for processing, handling, sharing, and collecting individual’s private data; and
- compliance with data privacy legislation.

3.29 The importance of data privacy

Global data protection legislation aims to give individuals control over their data, making sure that they know how their data is processed and utilised when it is in the possession of other organisations, and what further actions, and by whom, will be taken against their data. The legislation is designed by the judicial system of the country where the data is processed.
According to Data Privacy Manager (2020), in 2019 approximately 73% of consumers indicated that they had trusted in the organisations that handle their data matters more the previous year (2018); and that it could be assumed that trust levels have further decreased. It is for this reason that organisations must understand how to process and protect data belonging to individuals. Data owners expect this.

Data Privacy legislation has driven and enhanced the importance of data privacy. According to Reddy (2016), when businesses place an emphasis on data privacy legislation, while complying with data privacy legislation, they experience a positive impact on the business. In addition to this, the business can benefit from the following:

- improved cybersecurity;

- improved marketing;
- improved business risk management;
- improved customer experience; and - improved efficiency.

The GDPR, as legislation, has improved global data privacy practices. It is also a comprehensive and innovative law which has been widely accepted in the digital era. It has created modern ways to protect information in everyday data privacy practice. There are other stricter regulations, such as the HIPAA, CPPA, and COPPA, which define data privacy as a component which is different to data security. Therefore, data privacy is seen as compliance with data privacy regulations, with the focus on how to transmit and store data; while data security is related to practices and measures adopted in the process of preventing intruders, or any other external stakeholders, from the unauthorised accessing of data.

For organisations to comply with data privacy legislation and to protect data belonging to individuals, they need to have data security and data privacy in their organisations. The terms are similar, but they are different. Data security involves several standards and various measures and safeguards that block the exploitation of data, which was acquired though illegal methods, and involves hacking. Data security includes encryption, security on the network, and access controls.

3.30 Data transparency and privacy

Data is a new commodity. A company increases its value, based on the type of information it has collected from its customers (Data Privacy Manager, 2020). Hence, data is an asset for an organisation, and it is worth safeguarding. In addition to this, it is important for organisations to know that the data they have stored is borrowed from the owners, and it does not belong to them. Data owners have rights to data collected and stored by organisations; these rights allow data owners to request the deletion of their data, thus devaluing the organisation that held the data. It is for this reason organisations need to protect the data, cultivate the trust of individuals who own the data, and demonstrate transparency by engaging with data owners on how the data is stored, processed and retrieved.

A data breach has a severe impact on customer relationships. The two phrases, ‘data breach’ and ‘reputation’ are not best used in the same sentence. But there are instances where organisations are having to deal with these connected issues; especially organisations that do not comply with regulations (Data Privacy Manager, 2020). It is vital to understand that reputation management and trust are closely aligned. Thus, when a data-related incident occurs, it is affecting the bond between the customer and the organisation. When an organisation is hit by a data breach, bad press is inevitable. The customers may turn against the organisation because of bad press coverage. The details of the breach may land on social media, and the organisation will lose clients (Data Privacy Manager, 2020). A data breach reduces customer trust and confidence, and the organisation’s profits, value and reputation.

When a customer has data privacy, it means they have the right to be independent. Therefore, it is important for data to be protected, as the owner has the right to be left independently. The aim is not to hide, but rather to protect the independence of the data belonging to the customers. Data privacy legislation is binding and has been made available by the government. Governments world-wide have numerous data privacy laws to protect their citizens (Data Privacy Manager, 2020). The legislation is designed to regulate the data traffic of individuals and to heavily fine, imprison, or sanction violators of the regulations.

According to Data Privacy Manager (2020), Facebook budgeted an estimated $3 – $5 billion to deal with investigations levelled against them, which all relate to data breaches and inappropriately managing customers' data. This indicates that there is a visible price for lack of compliance for both big and small organisations. The average cost of data breach fines recorded in 2020 was $3.86 (Data Privacy Manager, 2020). In addition to this, data privacy legislation-related fines have cost organisations their reputations (Data Privacy Manager, 2020). According to FTI consulting (2020), an organisation affected by a data privacy incident will see a drop in its yearly turnover of 9%. The drop is closely linked to the organisation's reputation and loss of customer trust. An organisation that generates an average of $930 million in turnover will suffer an estimated loss of $79 million (Data Privacy Manager, 2020). An organisation may adopt various measures to clear its reputation. However, it will cost more than twice the amount of money to regain a lost customer. Furthermore, it is vital for organisations who have lost their reputations due to data leaks to accept that their pasts will always follow them. Most of their customers, who have access to computing devices, will search for them and will come across the bad media coverage related to the data breach.

According to Data Privacy Manager (2020), the average time it takes to identify a data breach is 280 days. Furthermore, it takes an average of $1 million to contain a data privacy-related breach in less than 200 days, and customer personal information has a cost of $150 per record (Data Privacy Manager , 2020). These are some of the reasons why data privacy legislation exists. Some data privacy regulations are outdated, in the sense that they do not cover the current trends in technology. In recent years, after the introduction of the GDPR, more countries have started to update their data privacy legislation; and GDPR is leading the way (Data Privacy Manager , 2020).

It is paramount for organisations to consider creating a business strategy and marketing plan which are suitable to address the changes in the data-driven era. The individuals who have data held by an organisation have the expectation that their data is protected (Data Privacy Manager , 2020). There are various benefits for organisations that align to the requirements stipulated in data privacy legislation. The benefits give the organisations a competitive edge, and an advantage within the digitisation arena.

According to Data Privacy Manager (2020), in 2019 the percentage of organisations that indicated that they had benefitted hugely by following data privacy legislation increased by 40%; and in 2020 a drastic increase of 70% was recorded. The benefits depend on an organisation's perspective and goals (Data Privacy Manager , 2020). However, the key benefits indicated are agility; investor appeal; innovation; brand value; and operational efficiency.

3.31 International data privacy trends

There is a long list of data privacy-related initiatives, which indicate that organisations are accelerating the transition in how they value and recognise an individual's data, with an improvement in how the data is protected and valued (Data Privacy Manager , 2020). Organisations which are thriving have already adopted data protection strategies for the future. The big four firms have their own challenges when it comes to data privacy. However, they try to secure customers' data and align to privacy legislation, thus positioning themselves as responsible. The CEO of Apple, Tim Cook, has given passionate talks about the data privacy legislation in the USA, focusing on reducing data collection, user consent, and data security (Data Privacy Manager, 2020). By 2022, half of the world's population will have its data protected by data privacy legislation, such as the GDPR (Data Privacy Manager, 2020). There is a trend for organisations to demonstrate transparency and compliance in how they handle customer data.

3.32 Fast-tracking data privacy regulation alignment

There is a massive exchange of data in the online space, and the revolution in technology is advocating for this exchange. Data privacy is the solution to administer this change. Data privacy legislation gives data owners the right to correct and be informed of their data. The government, through data legislation, is obliged to fulfil the rights of the data owners within a specific time frame. There are data privacy software solutions that are aimed at aligning organisations with compliance, through operationalising and automating data privacy standards (Data Privacy Manager , 2020). The data privacy software is there to assist with helping organisations to understand their data privacy levels, and improve them. The software provides some of the following functions:

- consent management;
- data owner requests; - revolution privacy;
  and - privacy portals.

3.33 Consent management

The aim of consent management is to ensure that customers' data requests are consolidated and managed. This process aims to improve customers' relationships with organisations. The requests made by the customers are therefore tracked and placed into a single data repository which is managed by the organisation (Data Privacy Manager , 2020). The consent agreed on by the customers are the data referred to here. The objective is to understand and analyse changes to the consent given by customers and to make it efficient for the organisation to process changes more effectively.

3.34 Data owner requests

A data subject is (the same as) a data owner. The data owners are key in the decision-making process regarding their data. In addition to this, they have more data rights than the organisation, even when the data is stored with the organisation (Data Privacy Manager , 2020). The data subjects'/owners' requests are designed to provide data owners with a platform to make requests regarding their data. Such requests pertain to data transparency, giving data owners access to their data. This portal is for data owners, specifically, to engage the organisation in possession of their data. The data owners' rights are regulated by the data privacy act, which means that users are given preference, over the organisation, regarding their data. Lastly, it is vital for an organisation to comply with the requests made by data owners, as they may be seen to be disobeying the regulations if they do not address the requests.

3.35 Revolution privacy (360)

This solution gives a comprehensive view of customers' data, indicating where the data is located, and how it is used and accessed. This solution allows the data privacy officer to analyse changes and patterns taking place regarding the data. The organisation can find indications of any unusual activity, so that they are able to react. The software allows the organisation to act swiftly and be decisive on issues that are related to the data they have collected (Data Privacy Manager , 2020). A benefit of the software is that customers and the organisation can have swift, transparent collaboration.

3.36 Privacy portals

These are the communication tools between the organisation and the customers. The customers indicate their preferences at any time. The organisation must adopt the preferences indicated by the customers. The customer might request data deletion, an amendment, or limiting the levels of processing by the third-party organisations (Data Privacy Manager , 2020).

The biggest challenge which calls for data governance and policies within an organisation are the data privacy regulations. The regulations introduce stricter operational, marketing and technological changes

and standards within the organisation (Data Privacy Manager , 2020). Furthermore, most companies do not have the insight to monitor, respond or track data subject requests or preferences.

3.37 Steps to consider after a data breach.

When organisations are challenged by a data breach they remain in the spotlight and it is difficult for them to make all the correct moves. However, they need to prioritise the following:

- Put everything on hold.
- Evaluate the situation.
- Reduce additional damages.
- Notify the stakeholders (data privacy bodies or customers).

Jeff Peters (2020) refers to information privacy as a sub-component of data security, which is the safeguarding of data, meeting security regulations, and obtaining consent from users. Data privacy has the following concerns (Peters, 2020):

- how data is stored and managed by third parties;
- how data is collected and disseminated legally; and
- data protection legislation, such as GDPR, POPIA and HIPPA.

Jeff Peters (2020) further highlighted that data privacy and security are the same thing, indicating that to achieve data privacy an organisation needs to adopt a data security platform. Dr. Cavoukian refers to data privacy as the freedom for individuals to have the space and right to reflect, and enjoy solitude and reserved moments (Privacy by Design, no date). Her role in the data privacy development process has increased her popularity, and her input now services modern data privacy legislation. Data privacy governs how an individual's data is collected, disseminated and used; while data security has the fundamental responsibility of protecting data from attackers who seek to access it externally or internally (Privacy by Design, no date).

Organisations generally believe that protecting data from hackers is sufficient and covers the data privacy legislation (Privacy by Design, no date). However, this is not the case. Internal attacks by disgruntled employees can pose a great risk to an organisation.

3.38 The importance of data privacy

According to Jeff Peters (2020), data is one of the most fundamental assets in an organisation. Data has become a commodity and organisations find themselves collecting, collating, disseminating and using data. Organisations like Twitter, Facebook, Google, and Amazon have created their wealth and empires

through data (Peters, 2020). Their data collection process must be transparent, and must adhere to all data privacy legislation. The aim behind consent is not only to legally adhere to legislation, but also to build trust with customers and partners who allow you to store and process their information. The majority of organisations have learned about data privacy through a difficult process where their data privacy failures are published.

Individuals have the right to privacy. This is a human right in some countries, and it is imperative for data subjects to be given privacy from surveillance. The definition by Laura, which indicates that data privacy is about how data is disseminated, shared and stored, shows that there is a clear and shared view about what data privacy is about (Privacy by Design, no date). Data privacy legislation also protects organisations from acting illegally. Some organisations collect information or data without consent, yet implement all technical measures to safeguard it.

When organisations ensure data privacy, they comply with consent and data privacy regulations. This makes the organisations appear to be responsible to the eyes of the customers (Peters, 2020). Some organisations use data collected to track users and then sell their sensitive information without the users' consent.

Employees in organisations must be trained in data protection on a regular basis so that processes and procedures are understood before any data is collected; and to ensure that the collected data is used according to the regulations and employees are acting within the correct boundaries. Information privacy also involves laws that are required for organisations to protect their data (Peters, 2020). There has been a consistent increase in data privacy legislation, globally, causing data privacy requirements to change and increase. However, data protection remains a constant, which is not affected by the changes. It is in the best interests of an organisation to ensure that they secure data belonging to subjects.

An article in Technically Positioned indicated that data privacy legislation is an increasingly important topic, globally. GDPR, again, appears to be the most comprehensive data privacy legislation, which governs data belonging to individuals in the European Union. More countries have followed by implementing similar legislation, such as the POPIA (Peters, 2020). The USA has generated a similar, comprehensive data privacy legislation in the CCPA, which was adopted in 2020, and shares common elements with the GDPR. The biggest commonality lies in the issues of informed consent, customers knowing how their data is used, and customers being the custodians of their own data, regardless of where it is stored.

The CCPA has encouraged other states in the USA to update their information security legislation, adopting the CCPA as a template. Another recent act which was passed in New York is the Stop Hack

and Improve Electronic Data Security (SHIELD), which elaborates on the issue of breach notification by organisations that are hacked. Organisations who store and disseminate data belonging to individuals do not enjoy the process of sharing data breach notifications. The rationale behind the SHIELD, by placing the emphases on data breach notification, is to primarily hold organisations accountable and indirectly force them to put in the necessary measures, such as physical and logical security.

The core advantages of the federal law are numerous. Firstly, federal data legislation could clearly articulate the comprehensive legislation at federal level, thus making consumers aware of their rights with respect to the data privacy legislation. As a result, citizens would know that they are entitled to have their data safeguarded, and organisations possessing their data are liable for any damages.

In addition to the rights of consumers to data privacy, organisations can benefit from comprehensive data privacy legislation which is developed at federal level. Another advantage of a federal law is that it would provide a streamlined frame of reference for businesses to adopt for compliance. In addition, this gives businesses a better position and understanding of the regulations, which can be shared with customers.

A compliant organisation automatically adds value to itself. Any organisation that conforms to data legislation which is comprehensive, is automatically able to understand the type of data it possesses, and which policies align. Thus, it will have a clear picture of how a user's data must be treated; what rights belong to the user; the data privacy protocols to adopt; and what measures can be adopted to minimise the risks.

3.39 Developing a compliance framework in a federal law

While government rules, regulations and guides evolve, it is anticipated that they will be extended and adapted to new trends that are dynamic, within the technological and data privacy space. Therefore, it is an excellent time for businesses to prepare for compliance and to build a foundation where existing, amended, and newly introduced legislation will be embedded. The growth in the information technology and artificial intelligence sectors will rapidly accelerate and affect changes to data privacy legislation. A recent example was announced in the European region in 2021, where the first ever artificial intelligence policy was put in place. As the changes occur, it is the responsibility of the businesses to follow and understand the changes as they appear. It is evident that any policy changes that are amended in the GDPR will affect other information security frameworks that are developed on the foundation of the GDPR. These include POPIA, CCPA and CPRA. When a compliance framework is developed, it must be supported by the foundation of comprehensive data privacy legislation. Definitely, compliance with a framework is simpler than compliance with a heavily texted policy or legislation. A framework is a condensed form of a regulation which speaks to low-level legislation. Business can easily adopt a

framework, to transition and align with privacy legislation. The USA is an area which is currently updating its data privacy regulations. When data privacy is updated, the country, federation or area can enjoy a robust data computing environment which affects its citizens positively.
Lastly, legislation that does not get updated is not in line with the ever-changing needs of society.

3.40 Information security resources

It is essential for organisations to provide employees with relevant information about security training and employ information security practitioners who possess updated information in the field. In addition, they should empower their security team with computing resources, knowledge, and certifications that will, in turn, increase the efficiency of the employees, thus strengthening the security infrastructure of the organisation. There are various information security-related courses which are aligned to the new data privacy regulations. The aim of the courses is to ensure that there is a foundation for data privacy practitioners to attain the knowledge that comes with change in the data privacy and information security arena. Some organisations have conducted extensive research in the security and privacy space, subsequently giving organisations the tools to leverage when improving their security efficiency. There are various tools and techniques that are used by hackers and various intruders. The tools and techniques aim to provide individuals with the knowledge to deter incidents of hacking, and how to manage incidents. These tools and hardware resources are there to remedy vulnerabilities. Organisations must fund the information security team and furnish resources to the respective teams so that they are able to tackle vulnerabilities. Management in organisations also needs to be trained in information security and to understand underlying concepts that are security related and affect the organisation. This empowers managers with the knowledge to provide their security teams with the necessary resources for managing the security aspect; and, most importantly, implement information security in the correct way.
While there are hackers who intrude, there are also hackers who seek to fix. These hackers are referred to as ethical hackers (Sobers, 2020). Organisations which have a wealth of information in their repository have the responsibility of making sure that they protect the integrity of the data. The responsibility lies not only at the operational level of the organisation, but also the senior level. Therefore, the skill of ethical hackers is vital in assisting organisations to identify their loopholes and cover their weak points. This is proactive information security. An organisation which is informed about their vulnerabilities can prevent what is known. An ethical hacker's report informs the organisations, and the knowledge assists with compliance. Lastly, when a hack takes place, the organisation needs to find ways to remedy it, and also find a way to restore what has been damaged (Sobers, 2020).

Web applications are the most vulnerable of an organisation's online assets. They sit in spaces which can be intercepted. There are various tools which are designed to penetrate web systems with the aim of stealing information belonging to customers. This information is as important to the hacker as it is to the organisation. Therefore, organisations must find ways to remove this threat. There are browser

residing plugins that are installed in users' computers. These plugins may either serve or sabotage the organisation. It is for this reason that organisations must be compliant and find ways to be proactive in implementing safe information security (Sobers, 2020). Lastly, they must ensure that these align to the requirements stated in the respective data privacy legislation.

There is a course for data security investigators which goes from basic to advanced. The most widely adopted data security solution is a network intrusion detection solution where data packets travelling on the network are analysed for suspicious activities. The team that uses the data intrusion detection needs to be trained on how to analyse data traffic (Sobers, 2020). There are various courses provided by the SANS, which are good at equipping the security employees with the competencies.
A popular social media mobile application, named TikTok, was issued with a record-breaking fine of $5.7 million when they were found to be in violation of the children's online privacy protection act by the US-based federal legislation trade commission, for their failure to obtain parental consent from minors who use the platform. Tik Tok is a Chinese-based organisation with a global footprint. However, their fine came from the United States of America (Sobers, 2020).

Most global web-based systems and mobile applications come from China, because of China's strength in the commercial, industrial, manufacturing, and tech-based innovation sectors. Therefore, China will have a footprint in most countries. As a result, China will need to align its data privacy laws with those of several nations (Sobers, 2020). Another popular Chinese mobile application, named Baidu, has been found to follow the least satisfactory data privacy protection mechanisms. However, other platform owners who are US- centric are more cautious and are committed to securing data belonging to their users (Sobers, 2020).

There is study that proved that Chinese-based web services have a negative record in the data privacy protection space. In 2006, prior to China passing its own data privacy protection law, there were 82 commercial websites that originated in China . Some did not have a data privacy disclaimer, while others did not follow the three core best practices for sites. In addition to this, most organisations who owned the sites did not store customers data in a secure environment, thus making them vulnerable to online data vulnerabilities (Sobers, 2020). Most South African-based organisations make business-tobusiness transactions with Chinese-based organisations. This encourages global trade and growth. Furthermore, some businesses in China have a business-to-consumer relationship with South African residents. The method of communication and transacting between the customers and the business is electronic. Therefore, the Chinese data privacy legislation must align with the POPIA. This is the case with any business which performs electronic transactions with countries in the European Union: they must have data privacy legislation that aligns to the requirements of the GDPR. Furthermore, they must endorse the GDPR, or they may be found to be guilty of non-compliance. Lastly, data privacy legislation cannot

be generic at the global level, as each own country has its own judicial system with different needs. Therefore, GDPR might be the best legislation for certain countries, while other countries find GDPR to be less impressive data privacy legislation.

Chinese mobile applications are globally accepted and recognised. Chinese organisations respond to varying government standards for data privacy in their global markets. There are four widely-used Chinese mobile applications: Baidu is a mobile web-based application with an in-built search engine component. Toutiao and TopBizz are news aggregators developed by ByteDance (Sobers, 2020). TikTok and Douyin are mobile-based applications that provide users with the functions to create short videos and share them. Lastly, WeChat and Weixin are social media mobile applications owned by Tencent and a Chinese internet company. The applications are recognised globally and have a large market footprint.

3.41 IOS and android differences

The registration steps between IOS and android on Baidu and WeChat differ. However, the registration steps for TikTok and TopBuzz are the same. The IOS process in Baidu and WeChat differs, as the IOS method has more steps than that of android. This means that the application requires more authorisation steps from the user with an IOS device. The android platform has installed several data authorisation steps as a default option. The IOS platform has a privacy option where the user of a device grants more authorisation for the application to make changes, and access certain data from the device, for matters of privacy. ByteDance, the owner of TopBuzz and TikTok, has set push notifications as a default option, which does not require any permission from a user (Sobers, 2020). In the event of a user wanting to block notifications, they need to go through their data privacy settings on their device to affect the changes.

3.42 The issue of consent with Chinese applicationlications

The applications have been set up to launch a pop-up window that contains and displays a detailed privacy notification. In certain countries, like Canada, this does not happen. The user needs to give consent to the pop-up launch; then they will get the privacy statement. However, in other countries, the application will not proceed to its other features until the user of the device has ticked a box indicating that they agree to the terms, conditions, and privacy statement for using the application. The terms and conditions, including the privacy statement, are accessible through a user-clickable link beside the check box that needs to be ticked. The user clicks that they agree, only if they give consent for the application and owner to use their data and make changes to the device settings, as mentioned in the data privacy statement.

Users who do not agree to the terms and privacy statement will not be allowed to access the features of an application. Martin (2013) stated that users who want to utilise parts of the application must be given an amended consent based on their requirements. This consent will cover portions of the application they want to use. In addition, give users access to utilising the application. However, the organisations do not have tailored consent notices for users with different needs. They view the application as a single entity that must be accepted or rejected as it is. In addition, these applications could ask users for specific information that generate a consent for which is custom, the information such as: do you want the application to collect your location history; if the users pick a disagree option, they should be able to use the application without sharing any location information, then the application should allow the user to proceed. Furthermore, the other privacy data required by applications do not necessarily require the user to consent to them for the application to function. While some other applications make it mandatory for the user to create an account and give a consent simultaneously before they make any access to any features of the application. Therefore, the user will only create have an account for the application only if they agree to the terms and privacy policy. While the other applications allow you to create an account and consent to any regulations thereafter.

3.43 User registrations

All the applications which have gone through the mandatory examination process provide users with registration options. A user can pick if they want to use a cell phone number or email address as their preferred primary key. The cell phone numbers must be international. However, for those who are local to the country where the application was developed, or data resides, the user is, by default, allowed to use their cell phone number without any consent approval challenges. These are key differences between the Chinese based TikTok/Baidu users and those in the international market.

China has made it mandatory for users to use their real names and email addresses when creating accounts. This is because they want to encourage good behaviour on social platforms, as they believe that users who use anonymous data to access social platforms tend to misbehave and make another legitimate users' experiences unpleasant. In addition to this, the application requires user behavioural information and location. Such data makes it easier for law enforcement and application owners to implement disciplinary measures for unethical behaviour, where necessary (Sobers, 2020).

The United States of America-based application and internet companies such as Twitter, Facebook, Instagram and YouTube have made it non-mandatory for users to give their authentic information when creating user accounts during the registration process. This means that a user may remain anonymous. Snapchat adopted a dual approach: users have the opportunity to create either an anonymous or a public account (Sobers, 2020). They have also indicated that public accounts are safer, as the users tend to

create a safer social media experience. In e-commerce space, users may create a fake account and procure items. Anonymous accounts introduce a variety of challenges for users on the internet.

3.44 Account deletion upon user request

A user may have their social media or e-commerce account deleted. However, this varies, based on the platform type and the organisation providing the platform. The user may be requested go through multiple stages to have their account deleted. WeChat has five steps, and TikTok has four steps. Organisations who have more steps tend to have a complicated approach to account deletion. However, when an account is flagged as suspicious for any illegal activity or for harming users, the organisation that owns the application has the power to suspend and delete the account, thus making the account inactive and unusable (Sobers, 2020). Some organisations, such as Alibaba, have given the users an opportunity to deactivate and delete their accounts within a set number of days. This assists users who have previewed the application and do not want an account with the organisation anymore. This process is called a pre-participation option, giving the user a higher level of control.

The need for standardised international data privacy legislation is great. This is because most application platforms do not have the required level of data privacy legislation to comply with the international market. Moreover, international users who come from countries where the data legislation is not covered make use of the applications complicated. An international standard will enable all continents to participate, and participating in drafting a reasonable and acceptable international data privacy act would make the legislative requirements for organisations that operate businesses on the internet easier. Thus, the world would be able to trade with a level of mutual understanding.

Data storage is an essential part of user data safety for the organisation that owns the application and web-based service. The country where the data is located must have reasonable data legislation which is acceptable to most parts of the region, if the application is regional, or international, and if the application is designed for the international market. The location of the data will be dictated by the geographical position of the market. For platforms such as Alibaba, WeChat and Baidu, the data is stored in Toronto, Hong Kong, and Canada, respectively. The application owners indicate the reason why the data is placed in these areas. In addition to this, the areas must have data privacy legislation which is widely acceptable.

All applications and websites for e-commerce must have a mechanism for users to indicate their concerns. This can be through email, telephonically, or on social media. The user, of their own volition, can request to be informed why their data is being moved or located in a specific area. In the event the user wants their data to be moved into another data-repository country, if the organisation offers data storage in that country, then, depending on the organisation, the data may be moved. The type of user

data ranges from contact information; addresses; banking profiles; preferences; and shopping information. This gives the users flexibility and a certain level of control when it comes to their data. However, the users are limited to the geographical areas chosen by the organisation that own the platform and services. A user requested that their biometrical information to be removed from a server located in an eastern country. The owner of the platform had to request the user to re-authenticate themselves on the platform, using non-biological features, thus fulfilling the request of the user, and enabling the user to have access to the platform via a password. It is for this reason that users need to understand the type of data collected by the applications they subscribe to. Lasty, users are the ones who control their behaviour on the platforms.

Data legislation and geography have always sparked debates on how the internet can be regulated, and how regulations that affect the wider geographical online market can be standardised. There is a banner dubbed 'internet sovereignty' by the Chinese government. However, data privacy and protection in China is state-centric, which means that the government governs data privacy independently, inclusive of internet-based data privacy (Simons, 2020). The Chinese government developed an internet data privacy policy which is inclusive of various government data privacy regulations, thus making sure that the data privacy legislation is inclusive. It was promulgated as the Cybersecurity law and was passed in 2016. This law is a big move for the Chinese to access and thrive in the international market. Most foreign organisations have reacted positively to the Chinese foreign promulgated cybersecurity regulation, including Apple, LinkedIn, and AirBnb. In addition, this the Chinese government requested that internet organisations enter into a joint venture with them to operate and store data on platforms such as Amazon, and Microsoft Azure cloud, to mention a few.

The Chinese government is involved in a wide variety of online transactions. These include, but are not limited to, data localisation specifications for local and international organisations. The Chinese government, like the European Union's GDPR, must have an understanding with international organisations that the data privacy legislation must align on most of the key points before they start making any web-based transactions (Simons, 2020). The aim of the government is to ensure that the users are safe and to protect users who are vulnerable.

The Chinese government has indicated that there is a growing need for data privacy for internet users. This trend is seen as a push from various government organisations on a global scale. In 2016, the Chinese government attempted to standardise their data privacy legislation and plays an active role in enforcing data privacy legislation that is standardised. In July 2019, the Chinese government had 16 national data privacy legislation standards, ten of which were local; while the remainder included international laws (Simons, 2020). Furthermore, 29 newly introduced data privacy standards were introduced to form a uniform and standardised data privacy framework. The joint legislation is seen to

be comprehensive, and satisfies the countries which generally create a lot of revenue for the Chinesebased organisations.

Organisations who own and operate applications utilise user data for several reasons. According to Simons (2020), when an application is given permission to collect data, whether regional or international, some organisations do not give a clear definition of how they will manage information that could identify a user, or personal identification information. Some applications indicate that they may share certain information with law enforcement agencies if required. Alibaba, on the other hand, has a strict local privacy policy; but they are less strict when it comes to international customers. This is because the Chinese government imposes certain rules on their own people. Other applications and sites have indicated that they will request the owners of the information for permission before sharing their data with any other third-party organisation. Therefore, a user will be made aware that their data is being requested and can either disagree or agree to this request. The Tok-tok platform has explicitly indicated, in their privacy policy, that a law enforcement agency will be given access to any data belonging to all users, upon a request.

China once reached the point where internet transactions were increasing exponentially. Mobile applications and websites were the major contributors. The cyber administration of China, which oversees cyber security space, started placing security measures on mobile application, because mobile applications were different platforms to web-based applications, even when they offered the same services (Sobers, 2020). Mobile application stores and web-based stores needed to have the same privacy standards, and at the start of 2016, they were governed the same in respect of data legislation. For this reason, mobile application developers must enforce the same data protection measures adopted on websites when developing mobile applications. There are different mechanisms for testing if data security mechanisms on mobile applications are the same as those on websites. The responsibility of the organisation that owns the mobile application is to display the data privacy regulations in the same way they are displayed on the web-based systems.

Most mobile-based applications make server-based requests to either search or exchange data. These are the same services that are accessed by web browsers when requesting data from database repositories. Mobile applications are also seen as devices which allow major data leaks, as users may have weak data security protocols, which make their server-residing information vulnerable. Mobile device operating systems have a layer of security to safeguard a device, including the mobile applications installed (Sobers, 2020). However, some users do not update their devices and end up with newly introduced applications, with new threats that cannot be removed by the device's operating system. Mobile application stores such as Google Play for android, and App store for IOS, do not approve mobile applications that cause possible harm to devices. Some users find applications from

illegal sites, or sites which are not approved by the mobile application operating system. In this case, the user grants the application the rights to make modifications on their phone, thus compromising the device and leaving it vulnerable to hacking (Sobers, 2020). This proves that users have a vast amount of power over what they approve and do not approve on their primary devices.

3.45 Cybersecurity during the COVID-19 pandemic

As countries across the world were affected by the covid-19 pandemic, governments enforced a lockdown. The lockdown was introduced to curb the spread of covid-19 infections. However, cybercriminals also found a space to operate as they sprang into action. In South Africa, during the first 100 days of lockdown, the number of spam attacks increased up to 45%; malware spiked by 385%; and impersonation attacks went up to 75% (Mimecast, no date). This research was conducted by Mimecast. Most organisations who offer professional services provided their employees with equipment to work from home. The equipment was an internet connection, and computing devices (Mimecast, no date). The number of cybersecurity attacks soared during the time where employees were working from home. While certain companies have started phasing employees back into the offices, those who are working from home are still affected; and the attacks are most likely to increase as time goes.

Mimecast conducted an online survey for companies during the pandemic. Approximately 45% of the respondents indicated that most of them were affected by the ransomware attack. Successful attacks usually result in system downtime and data loss, which affects organisations' revenue. A subject matter expert in Cybersecurity spaces, Duane Nicol (2019) indicated that the number of cyber security-related incidents will continue to increase. Ransomware will be the biggest security vulnerability, affecting organisations and global networks will be compromised. The growing trend in ransomware is not only money, but anarchy. In 2020, there was an attack in a Germany-based hospital, where the intention was to delay a patient from receiving medical attention timeously, Duane Nicol (2019). As a result, the lady lost her life. Some have labelled this incident as the first cyber-attack-related death.

Law enforcement agencies have made progress in blocking some gangs that deal with botnets and ransomware. However, cybercriminals always find a way to introduce new threats. It is evident that the threats are removed after the damage has been done. Therefore, a much more proactive information security strategy needs to be employed to remedy the attacks (Mimecast, no date). A proactive approach will reduce the number of active threats, or delay the greatest impact a threat may cause. It is predicted that cybercriminals will also find ways to capitalise on the covid-19 vaccination rollout. A US-based vaccination cold storage company has already been affected by a ransomware. This proves that the cyber-attacks must be monitored.

3.46 Remote workers are cybersecurity targets

The work-from-home strategy employed by corporations to keep their businesses running has become a primary target for cyber attackers. In 2021, we will continue to see more work-from-home-based attacks. Home-based networking has a greater level of vulnerability compared to office-based networking. These vulnerabilities will lead to attacks that will affect the business continuity of organisations who have home-based working teams. Most smaller organisations do not have the financial resources to deter most threats (Mimecast, no date). Larger corporations will need to expand their information security budgets so that they are more able to deter risks and keep their business reputations.

3.47 Focus on cybersecurity training and awareness programme

In 2021, security awareness training should be in the spotlight for organisations. This is one of the best approaches organisations can adopt to enhance their employees' security awareness, and should yield great results, as their staff members will become the firewall against threats that come directly to them. Mimecast also conducted research in South Africa, and the results indicated that email security threats were prevented by employee awareness about email security. Some employees agreed to having opened suspicious emails, but the majority claimed that they managed to avoid and delete the emails (Elin, 2020). Therefore, training and awareness programmes must be conducted regularly.

The information and cybersecurity teams in organisations will be forced to adopt a more practical hacking strategy to assist employees in organisations understand how these threats present themselves. This will increase their awareness and assist employees, who are working remotely, to handle the situations in a way that will benefit the organisations (Elin, 2020). This means that remote-based employees will have their computers injected with server-based attacks, and they will have to understand how to avoid them. These attacks usually come as emails from legitimate subordinates or customers, but with the intention to break into the system.

Reports of breaches have increased since the POPIA legislation.

As of July 2021, South Africans will have noticed an increased number of headlines relating to information security breaches. This is because massive data breaches have been reported to the information regulator. Most of these breaches highlight the weaknesses in organisations' security measures. The courts will have to handle more cases that result from the data breaches. The POPIA breach notification clause forces organisations to disclose data related security breaches (Elin, 2020).

3.48 Cloud-based system protection for the public sector

According to Thomas Mangwiro (2020), who oversees Mimecast's public sector portfolio, cloud-based systems enable agility in the public sector in South Africa. Furthermore, Thomas indicated that the

public sector would require a vast amount of support as they migrate to cloud-based technology, and they will rely on partners who have the skills to remedy risks and vulnerabilities on the cloud-based systems (Elin, 2020). As the migration to the cloud grows significantly, new strategies will need to be adopted to ensure compliance with the POPIA regulations, and for the government to have sovereignty over data. The benefits of cloud-based systems are great and outweigh the risks of security threats. This means that the public sector South Africa will need to be more efficient on issues pertaining to service delivery. However, many will be confronted by outages and system downtime, which could also, potentially, lead to a widespread disruption of national systems that are critical. This issue may present itself if the government departments use the same cloud service provider, and the vulnerabilities and threats emerge as new technology is adopted (Elin, 2020). There is no single method to avoid threats. The only solution is to invest in security tools, teams, and techniques. This shows that the POPIA legislation and its requirements will change as technology changes.

3.49 Cloud providers and the POPIA

SMEs and other forms of business who trade within the e-commerce space have seen a new trend which surrounds how data is stored and processed. The new trend refers to the cloud. The cloud can be adopted in many forms, such as: storage, hosting to name a few. With this new trend, organisations find it convenient to migrate to the cloud, and also leverage from benefits absorbed from such storages. As a result, businesses would be compelled to collect data from customers and share it with third-party cloud providers (PaySpace, 2021). However, they need to still uphold and respect the requirements indicated on the POPIA legislation for any organisation contracted to be the cloud provider. In addition to this, an organisation that seeks to use an international based cloud provider, would need to be aware of the POPIA, and follow the requirements which are indicated in the legislation. Moreover, the issue of consent plays a crucial role, as customers who have their data stored externally would need to be informed of this (PaySpace, 2021). Lastly, cloud providers would need to also find a way to be compliant with the legislation, such that they enforce stringent data security protocols which speak to the needs indicated in the 7th condition of the POPIA. These technical measures must protect the customers data. The very same way, a data subject is a customer to an organisation using cloud hosting services, the cloud hosting services needs to treat the client organisations data as their data subject and reference the POPIA requirements. A written contract which governs what the cloud provider can and cannot do when handling the data, must be signed by the client organisation (PaySpace, 2021).

3.50 Organisational culture

Organisational culture refers to a set of living relationships working together towards a shared goal, it is not something that you are, it is something that you do (Randhawa, 2019). This means that an organisation sets boundaries and values that drive the work attitude in action. Organisational culture

sets the climate for an organisation. In addition to this, it is an investment to the organisation in that it seeks to instil principles, values, and ethos that protects its vision, mission, and external judicial requirements such as the POPIA, and also push towards driving overall business success (Randhawa, 2019). An organisation which has a respected and adaptable culture find it easy to maintain its vision and make amendments where required. In respect to the POPIA, organisation culture would play a crucial role. The POPIA in alignment to the SMEs organisation culture would mean that an organisation needs to make a space within its operations to uphold and respect the POPIA legislation. Furthermore, management would support this vision through providing staff with educational programs, signing of agreements that enforce employees to oversee, and implement the POPIA in their daily duties, and system development for the e-commerce sites. The organisational culture aspect would strengthen the process of POPIA implementation and maintain the momentum. As a result, an organisation would align with the legislation. In closing, the POPIA would be built into the organisation culture for a sustainable implementation.

3.51 Conclusion

This chapter has introduced the concept of information security and its relationship with the POPIA in detail. It also investigated information security and information security management systems. In addition, it has reviewed literature that focuses on the data privacy legislation locally and globally, and how it affects businesses; the types of attacks that affect businesses that do online-based transactions; and challenges introduced by intruders.

Furthermore, the chapter reviews information security at the local and global scale, looking at what other continents and countries are doing to respond to data privacy legislation. It considers the different types of information security threats and how they are managed through technical control and management measures.

The next chapter covers the research methods, data analysis and design adopted to meet the objectives of the research paper.

CHAPTER 4: RESEARCH METHODOLOGY

4.1 Introduction

Research methodology, as defined by Kotari (2011), refers to the process adopted to scientifically solve a research problem. There are various steps, techniques and procedures adopted by a researcher to address a research study, including day-to-day procedures, for addressing and analysing a research problem. Therefore, this chapter discusses the research method; research design; research procedure; sampling method; population; data collection instrument; and data analysis procedures adopted in this study to achieve the objectives of this study and develop a framework which is useful for SMEs to use as a frame of reference for POPIA compliance.

The intention of this study was to develop a frame of reference for SMEs to leverage when aligning to the conditions of the POPIA. Therefore, the research problem and research questions guiding this study were developed so that they influenced the development of such a framework. According to McCombes (2019), there are numerous research designs. However, each research design aligns to a specific research paradigm. The three main research paradigms are mixed methods, qualitative, and quantitative (McCombes, 2019). Exploratory research work aligns with a qualitative paradigm, which is adopted for developing an understanding of opinions, underlying reasons, and motivations (John Dudovskiy, no date). Quantitative research, on the other hand, seeks to uncover insights, ideas and trends, and may also look deeper into a problem (McCombes, 2019).

Structured and semi-structured interviews are used as a data collection method for a qualitative study (Doyle, 2020), whereas, a quantitative study makes use of numerical data, and statistics to turn it into useful data, to quantify a problem. Quantitative research is used to quantify beliefs; opinions; behaviour; attitudes; and other variables defined to generalise the results produced from a sample to a population (DeFranzo, 2011)**.**

According to Schoonenboom (2017), mixed methods refer to a method where quantitative and qualitative data collection and analysis techniques are adopted in different phases of a study. Such phases can be undertaken sequentially or concurrently (Schoonenboom, 2017). The world view perspective, in addition to the researcher's intuition, guided the research design for this study. Furthermore, the quantitative nature of this study is descriptive and is not limited to any theory. The study used a questionnaire to elicit information from participants on how consultants or employees in particular SMEs implement information security practices which speak to the POPIA. Therefore, from the specifications above, a descriptive survey is the most appropriate design for this study.

The descriptive survey was conducted in a single phase, where a questionnaire was sent to the participants. This is quantitative data collection and analysis. The output from this single phase guided the researcher in understanding what SMEs are doing, and the types of challenges experienced by SMEs using e-commerce platforms when implementing the POPIA, as well as the knowledge they could contribute to creating the frame of reference (Schoonenboom, 2017). This knowledge was used in the development of the framework for implementing the 7th condition of the POPIA in the SME ecommerce sector. Therefore, parts of the framework are based on SME knowledge of information security, and the appropriate practices that these SMEs adopt in aligning to the POPIA. This process was also guided by the theoretical and conceptual frameworks known as COBIT 5, ISO 27001/27002 and NIST SP 800.

4.2 Research paradigms

Mackinnon and Powell (2008) describe a paradigm as a set of beliefs that can be regarded as a worldview on how scientists agree to address and solve problems (Mackinnon & Powell, 2008).

A paradigm contains four elements: methodology, epistemology, ontology and axiology (Mackinnon & Powell, 2008)**.** It is vital to have a deep understanding of these elements because they contain the key beliefs, assumptions, values, and norms contained in each paradigm (Žukauskas, Vveinhardt & Andriukaitienė, 2018). The norms, beliefs and values in the paradigms must be upheld in the research. Therefore, it is vital that each of these elements is understood and distinguished. Epistemology places its focus on the relationship between the participants of a study and the researcher, whereas ontology refers to the form and nature of reality, and what is known of it (Steup & Neta, 2005)**.** Positivism and post-positivism, and constructive and critical theories, are evidence of the existence of multitude paradigms (Steup & Neta, 2005). The objectives of post-positivism and positivism are primarily explanatory. Critical theory, on the other hand, provides a critique; whilst transformation and constructivism aim to provide an understanding and reconstruction in the area of enquiry (Willis, 2017).

Philosophers support the pragmatic paradigm, stating that it is not possible to attain a ‘truth’ about the ‘real world’ by limiting researchers exclusively to one scientific method, as prescribed by the positivist paradigm (Giacobbi, 2011). Furthermore, the philosophers claim it is not possible to determine social reality using the interpretivist paradigm. Rather, the pragmatic paradigm allows the adoption of one either the quantitative and qualitative research method; and the researcher can use the one which fits their study under the pragmatic paradigm. Thus, the pragmatic paradigm is best suited for this study, as it gives the researcher the flexibility to use any method to conduct the study.

In this study, the researcher uses a single method because mixed methods are time consuming; expensive; have a complicated research design; and are resource-intensive. Furthermore, the qualitative method is not suitable for this study because the study is quantitative in nature. Moreover, a quantitative

approach is most suitable because the study uses a questionnaire for data collection, it is not subjective and generates knowledge in an area that has not been researched extensively or objectively.

The researcher decided to use one methodology to compile knowledge to create a framework which could be adopted to implement the 7th condition of the POPIA in the SME e-commerce sector, and to assist SMEs with POPIA compliance. This preference for one approach is also based on the pragmatic realism philosophy, where a topic of contention is explored by the researcher using 'real world' organisations in the problem domain. For this study, real world organisations are represented by the SMEs and employees, and consultants who play a role in assisting the SMEs develop their e-commerce platforms and learn about POPIA.

For a conclusive study giving the best interpretation of the results, and an understanding of the phenomenon being studied, a quantitative research approach was adopted. The quantitative research approach was chosen because it enabled a detailed investigation for the development of a frame of reference that would aid POPIA implementation in SMEs. Furthermore, it provided us with an exhaustive process to achieve the objectives of the study.

A questionnaire was the primary, and only, data collection tool in this study. For this study, data was collected through a self-administered questionnaire, and the questionnaire was electronically distributed by the researcher. The questionnaire was developed by the researcher and literature was used as a guide for developing the questionnaire. A quantitative research approach suited this study. A quantitative approach is an objective, systematic, formal procedure of describing and testing relationships to examine causality and effect between variables (QuestionPro, 2018).

4.3 Research design

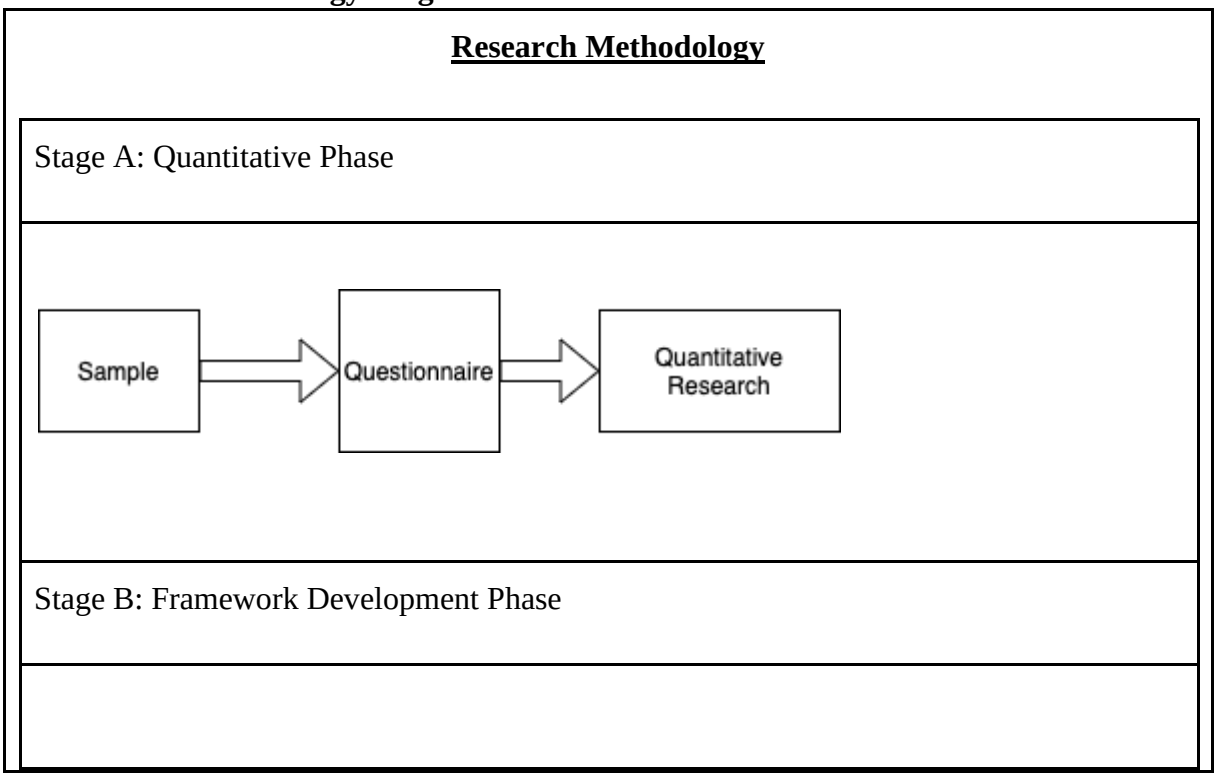
Research can be causal, exploratory, or descriptive in nature (Rvarughese, 2016). Descriptive research is quantitative and utilises a survey to collect data from a population. It focuses on answering the how, where, or what of research questions, and not the why (Mcleod, no date). Causal research has similar characteristics to descriptive research because it is pre-planned, quantitative, and focuses on a population. However, causal research, as opposed to the observational method in descriptive research, focuses on uncovering the cause-and-effect relationship between variables (Mcleod, no date).
Exploratory research is different from causal and descriptive research because it is qualitative and focuses on uncovering insights and discovering ideas.

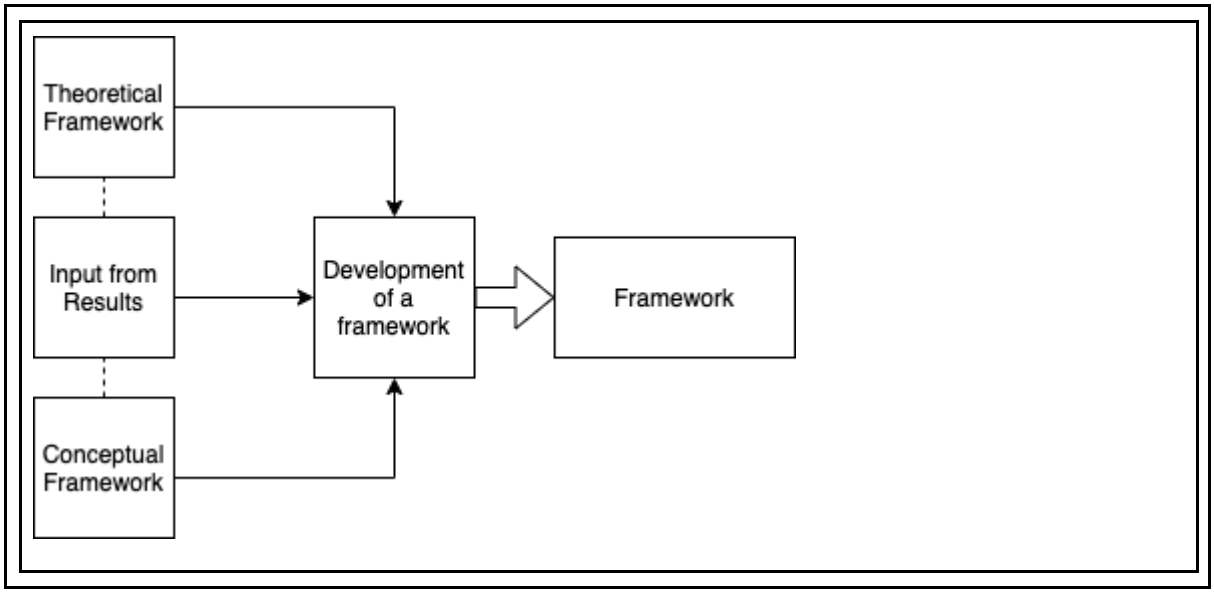
Research methodology can be associated with two possible research approaches: A qualitative approach is subjective, and seeks to assess attitudes, behaviour, and opinions (Damaskinidis, 2017). A

quantitative approach, which is objective in nature, focuses on developing new data, which is analysed quantitatively. According to George Damaskinidis (2017) quantitative research is inferential. This means that the population is observed, or questioned, in the study, with the aim of generating characteristics that can be generalised to a population.

A descriptive survey was adequate for this study because it yields an accurate portrayal of the opinions; abilities; beliefs; characteristics; and knowledge of the sample (Hale, 2011). Furthermore, the research methodology suitable for this study is descriptive in nature, as it addresses the research questions and objectives of this study. Lastly, the nature of this study requires a quantitative inferential research approach; and survey questions are suitable for this.

4.4 Research Methodology Diagram





4.4.1 Stage A: Quantitative Phase

The quantitative stage consisted of obtaining results from the sample. A questionnaire was the method adopted. It was sent as a link through email, and WhatsApp, to reach the sample; and the sample used their smartphones or laptops to provide answers to the questionnaire. This completed the quantitative phase of this study.

4.4.2 Stage B: Framework Phase

Stage B, in the diagram, shows that a theoretical framework, a conceptual framework, and the study results were married to produce a framework, as indicated by the objectives of this study.

The fundamental output of this study is a framework for implementing condition 7 of the POPIA. COBIT 5, ISO 27001/27002 or NIST SP 800 strengths are adopted in developing this framework. COBIT 5 has sub-processes that are well- suited to filling the gaps in ISO 27001/ ISO 27002, and NIST SP 800 is used in implementing GDPR.

For this study, the researcher used the outcomes of the questionnaire to suggest two of the most preferred theoretical and conceptual frameworks, as well as the most preferred, correct processes that align to the 7th condition of the POPIA; thereby developing a framework that enables SMEs in the ecommerce sector to be POPIA compliant.

4.5 Research Approach

This study used a quantitative research methodology, with the aim of uncovering current practices and understanding what is generally done, and how it is done, to ascertain the variability of a solution. This

approach was motivated by an established research methodology known as descriptive research. The chosen approach works, along with quantitative data, to understand the domain studied and to develop a possible solution to achieve the objective of this study, by developing a plausible framework for the 7th condition of the POPIA, which SMEs in e-commerce can utilise when seeking to align their IT systems with the legislation.

According to Streefkerk (2019), qualitative and quantitative research are the two main research approaches. The methodology is dictated by the kind of data collected by the researcher; the method used in data collection; the analysis; and its presentation (Streefkerk, 2019) . Quantitative studies assess samples from areas of interest and describe the relationships between variables. Furthermore, they use statistics, such as relative frequencies, to analyse the correlations and differences between the variables. A qualitative study, in contrast, predominantly uses data collection strategies such as interviews; participant observations; observations; manuscripts; official documents; responses and researcher views; or a data collection method that generates and analyses non-numerical data (Hashmi et al., 2017).

4.6 Study Site

Gauteng is the province with the biggest migration from other South African provinces. It offers more employment and business opportunities, and it houses the most economically productive square meters in Africa. The population is estimated at 15.7 million and it is the smallest province in South Africa (Isaca, 2014; Rogerson, 2018). The population for this study was in Johannesburg and Pretoria, the two major cities where the sample with the required skills is known to be located. Furthermore, the researcher resides in Gauteng and has greater access to the population and sample. For this reason, the researcher chose Gauteng as the study site.

4.7 Target Population

According to Krieger (2012), a population refers to a group of people, or objects, in which the data analysis is conducted to meet the objectives of a study (Krieger, 2012). The targeted population of this study included information technology practitioners who were involved in the information security aspects in South African small and medium enterprises. These practitioners operate from the ecommerce IT sector. These experts could provide feedback to meet the objectives of the study, and they were within the researcher's reach. In addition, the information technology practitioners make up the team that needs to be technically involved in implementing the POPIA and systems built or used by the organisations. This population was also easy to access because SMEs do not have the restrictions of large corporate organisations, which could have delayed or prevented the researcher from conducting the study. The sample for this study consisted of 86 participants

The targeted population for this POPIA research survey were employees or consultants who worked for, consulted with, or assisted in developing an e-commerce application for, SMEs based in the Gauteng province of South Africa. The type of work done by the consultant or employee had to be linked to software engineering; database development; information security; or directly to the development of the web application e-commerce platforms which are owned by the SMEs. The questionnaire in this study required such participants as they have the knowledge required to provide the information requested by the survey.

4.8 Sampling Strategies

Sampling refers to the process of selecting a portion of a full population (William, 2016). The portion must represent the actual population it was extracted from. This process is referred to as generalisation (William, 2016), and allows the researcher to gather information that meets the objectives of the study. A simple random sampling method is the process of randomly selecting a sample from a population, with the intention of giving everyone in the qualifying population a fair chance to participate in the survey.

According to Faber (2014), a bigger sample reduces variations and increases the chances of the research giving a more accurate outcome. Researchers, in general, may be biased in determining a sample size, and in measuring or choosing a healthy and significant sample. For example, when they estimate the population size for an area of research of interest to them, they pick regions where the sample is well suited to their research, as opposed to selecting the entire population with an equal probability (Faber, 2014). To reach a more precise estimate of the population size, the sample must come from areas with a fair representation of the population, meaning that the numbers must be proportional to the population. A simple random sample has the benefit of reducing bias and giving all the participants an equal opportunity of participating in the sample (Horton, 2020). The selection of areas to be sampled in a simple random sampling can be facilitated by a random number generator. These random number generators can generate a random list of numbers, indicating participants or places to sample.

The sample for this study was limited to the individuals who were employed, or consulted in work, for SME e-commerce systems development; who understood the POPIA; and who were based in Gauteng, South Africa. The role performed by the employee, or consultant had to be closely aligned to the development of the actual e-commerce solution, software engineers; database developers; information security specialists; and data controllers. In addition to this, to entrench the sample's validity, the sample had to be informed on the POPIA legislation in general and have knowledge of the 7th condition of the POPIA in detail. This ensured that the researcher could achieve the objectives of the study.

4.9 Sample Size

A sample size must be carefully determined for it to be adequate and yield a generalised and valid inference (Singh, 2014). The problem under investigation must provide information on the acceptable determination of the sample size, drawn from the population in the study. Furthermore, the subclassifications for the sample must be cost effective, precise, and available to analyse and investigate. A questionnaire was the only tool used to collect data for this study. The questionnaire was designed, based on the objectives of this study, to ensure that the data collected met the objectives of the study.

A sample is an essential feature in any study that seeks to make general inferences about the population it was extracted from (Horton, 2020). Furthermore, a sample size that is used in any study is determined by the cost of collecting the data, and statistical resources. Some studies are advanced in nature and may have several sample sizes to reach the objectives of the study. In some survey studies, if a population is heterogeneous and contains stratified sampling, there would be different sample sizes, based on the population they were extracted from. A complete enumeration approach is used in a census when collecting information. This is when the sample size and the size of the population are equal. However, experimental studies are composed of groups which are partitioned off, with each section containing a different size for each group that is used in the experiment (Singh, 2014).

Several considerations are used to determine a sample size. Such considerations are, but are not limited to, availability of the sample (Is the sample readily available?) and the cost. Furthermore, smaller samples, even when desirable under certain circumstances, may yield hypothetical statistical errors. According to Creswell (2017) sample sizes are generally predetermined by the quality of the resulting estimates, and a sample size may be measured based on the strength of the hypotheses test output (Creswell, 2019).

This study used a quantitative methodology. The sample was drawn from the Gauteng province, predominantly in Pretoria and Johannesburg; limited to information technology employees, and consultants who work in building e-commerce systems, with an understanding of information security; working in data analysis, software engineering, database development, and information security; or with a direct technical link to developing the security logical side of the e-commerce application, for a small or medium enterprise. These participants were chosen because of their knowledge and experience and involvement in working on projects that are linked to SMEs and e-commerce.

The population list was partly drawn from a conference delegate list, where only SMEs running ecommerce-based businesses were invited. In addition, the delegates contacted us with other SMEs who operate on e-commerce applications. The core objective was not to generate any generalisation of external validity of the results. However, the aim was to develop a frame of reference that can assist

SMEs in achieving the requirements stated in the 7th condition of the POPA. The main requirement to participate in the sample was the necessary skill set; living in the area; involvement in developing ecommerce for SMEs; and understanding information security and its elements. These skills are limited to information technology practitioners in general. These selection boundaries or criteria are a result of the sample and population being able to address the objectives of this study, so that the sample size, including the outcomes, could be accepted with a high level of confidence.

The choice of this sample size was based on the researcher's ability and access to the respondents. Furthermore, a sample size of more than 50 improves the chances of obtaining a fair distribution. However, in the event that the sampling test does not meet the normality test, then a nonparametric method containing measurements like the median, can be adopted to derive an aggregate representation of the data sampled. For this, correlation analysis was conducted using Spearman's correlation coefficient.

4.10 Data Collection Methods

Data collection refers to a method or technique used to collect and evaluate data collected on variables being studied, by adopting a recognised procedure, which allows the researcher to test a hypothesis, answer the research questions, and formulate and evaluate responses (Gill et al., 2008). A vital element of the research design is the data collection. If an incorrect approach for collecting data is used, then the outcomes of the study will be distorted. There are various data collection methods, each with their strengths and weaknesses. However, the most-used data collection methods are observations, questionnaires and interviews (Gill et al., 2008).

For the purpose of this study, and to achieve its objectives, the most appropriate data collection method was a questionnaire. The questionnaire was distributed to 86 respondents of interest. The questionnaire was used to collect the quantitative data for this study. The questionnaire was distributed electronically, and participants were asked to complete and return the questionnaire within a specific time frame. A questionnaire is good method of collecting data because (Institute of Lifelong Learning, 2009):

- they ensure a higher response rate;
- the researcher collects them personally;
- they offer a degree of anonymity;
- administering questionnaires is not too taxing; and - there is a less likelihood of bias.

Three major phases constituted the data collection plan for this study: an ethical clearance application from the University of Kwazulu-Natal; an informed consent from the participants; and a gatekeeper's letter which was issued to all the SMEs that met the selection criteria.

4.11 Interviews

Data collection using interviews requires face-to-face interaction. Under certain circumstances, interviews may also be conducted telephonically or virtually through online platforms for communication (McGrath, 2018). Interviews can either be structured or semi-structured (McGrath, 2018) . Interviews allow the researcher to collect data and gain deeper insights during the interview process (McGrath, 2018) . On many occasions, interviews are suitable when the researcher seeks to develop more understanding of the subject matter and enable the respondents to express themselves and describe their in-depth experiences (McGrath, 2018). However, interviews require substantial resources, including time and money to conduct them. This is a very real disadvantage of interviews, especially when the size of the sample is large (McGrath, 2018). Therefore, because of the disadvantages indicated above, interviews would not be an applicable data collection method for this study.

4.12 Questionnaire

A questionnaire was the main data collection instrument used in this study to gather information on how the SMEs, e-commerce and IT practitioners work towards compliance with the 7th condition of the POPIA, which is the pressing issue as it is South Africa's new data protection legislation. The researcher used a questionnaire and distributed it to the sample. Use of a questionnaire allowed meaningful quantitative data analysis; and given the large sample size, it was more practical to use a questionnaire with short-ended questions. This questionnaire approach aligns with the objectives of this study, which is the reason the researcher chose the questionnaire option. A questionnaire was a suitable approach because (Picincu, 2018) :

- they ensure a higher response rate;
- the researcher collects them personally;
- they offer a degree of anonymity;
- administering questionnaires is not too taxing; and - there is a less likelihood of bias.

4.13 Data Quality Control

Validity and reliability, or data quality control, refers to the key subjects to be monitored and evaluated. According to Chiang, Jhangiani and Price (2015), validity refers to the ability of the study to evaluate what it is intended to, and its alignment with the data analysis to reach the objectives of the study. The chosen design of a study must be able to provide responses to the research questions and fulfil the objectives of the research. This is the process of upholding validity in a study (Chiang, Jhangiani & Price, 2015). For this study, the validity of the quantitative data was in selecting a population and sample which was experienced and with the required knowledge to respond to the questionnaire. From an analysis point of view, the validity of the quantitative data analysis was maintained through adopting recognised processes of quantitative data analysis, such as statistical analysis, and data triangulation

(Chiang, Jhangiani & Price, 2015). Furthermore, participants were given a chance to provide feedback. Reliability refers to the credibility of the outcomes of a study: Are the outcomes derived from this study generalisable to a maximum or minimum extent, maximum being good? The reliability of the quantitative data collected was measured using the Cronbach alpha test. Furthermore, a pilot study was carried out, using the questionnaire. This test allowed the researcher to assess

- how subjects react to questions;
- if the questionnaire is understandable; and
- if the more questions need to be added, or some omitted.

4.14 Tests adopted in the study:

- descriptive statistics including means and standard deviations, where applicable. Frequencies are represented in tables or graphs;

- Chi-square goodness-of-fit-test, a univariate test, used on a categorical variable to test whether any of the response options are selected significantly more/less often than the others. Under the null hypothesis, it is assumed that all responses are equally selected;

- binomial tests test whether a significant proportion of respondents select one of a possible two responses. This can be extended when data with more than two response options is split into two distinct groups; and

- one sample t-test, which tests whether a mean score is significantly different from a scalar value.

4.15 Data Analysis

Thorne (2000) states that qualitative data analysis allows for valuable insights to be gained by a researcher, who has access to a vast number of conclusions from the collected data. Qualitative data analysis borrows from techniques such as narrative analysis; content analysis; relational analysis; and conceptual analysis (Thorne, 2000). These techniques each different, with each having its own strengths. However, none of these approaches is useful in this study because it is not qualitative.

Correlation analysis of the quantitative data collected in this study was conducted using Spearman’s correlation test. In the event that the Shapiro Wilk normality test proves that the data is normally distributed, then statistical analysis is applied. To measure the reliability of the inter-item reliability of the data generated by the survey, the researcher used Cronbach's alpha. The IBM SPSS data analysis software was used for the data analysis.

4.16 Ethical Considerations

The University of Kwazulu-Natal's ethical standards were addressed to ensure that the research conforms to the institution's requirements. An ethical clearance application was submitted, and clearance was obtained from the University of Kwazulu-Natal's Ethics Committee to grant the researcher permission to conduct the study. Gatekeeper's permission was obtained from all the SMEs who make up the population of this study. The researcher also obtained consent to conduct the research from the SME participants and a consent form was distributed to all the respondents for their consent. The participants have been clearly informed of how their data will be utilised and processed, and consented to giving the researcher access to their data for the study.

Anonymity and confidentiality for this study were addressed with the participants. The participants were informed that their personal and employment information would not be shared or be available to anyone. Furthermore, to ensure anonymity the researcher did not collect any personal information that might be used to identify the participants. For this study the researcher managed to obtain 76 gate keepers' letters.

1. The participants were not subjected to any form of harm.
2. The participants were all treated with dignity and respect.
3. The privacy of the participants was assured.
4. Participation was voluntary.
5. At no stage was there distortion or any form of exaggeration in this study.
6. The questionnaire does not include any discriminatory, offensive, or unacceptable language.

4.17 Conclusion

This chapter discussed the research method used in achieving the outcomes of this study. A high-level research design was discussed in this section, as well as the data collection, sampling, and statistical techniques for analysing the outcomes. Furthermore, the chapter provided details on how sampling was conducted and how the questionnaire was distributed to the participants. Due to the large size of the population, a sample was used.

4.18 Limitations of the study

The findings of this study can only be applied to areas from where the population which made up the sample was selected. Furthermore, due to budgetary and time constraints, the researcher was not able to add other business sectors (hospitality, tourism, medicine, other bigger business sectors) to the study. Therefore, the study is limited to the SME's commerce division where the sample has been selected. Lastly, due to the COVID-19 pandemic and lockdown regulations which affected the study, the researcher was limited to electronic means to collect the data. The questionnaire was self-administered.

CHAPTER 5: DATA ANALYSIS

This chapter presents the discussion of the findings of the study. The researcher adopted a quantitative research method in conjunction with a descriptive survey design to collect data from the study participants. A single questionnaire was shared with the data subjects, who consisted of IT professionals who perform IT functions in SMEs. The data was collected from participants who work within Gautengbased SMEs, and work in IT functions to develop e-commerce sites. The sample consisted of 86 participants. The data was gathered through an online questionnaire, due to the restrictions during the covid-19 pandemic. The data collected was electronic and was analysed using a computer program, SPSS. The research outputs are presented using frequency tables, bar graphs diagrams, frequency counts and percentages.

5.1 Demographic information

In this section, the demography of participants is addressed, looking at gender, age, job role and core functions performed, as well as work experience within the sector. Their practices and awareness of POPIA legislation are then presented.

Information regarding the demographics of the sample, both personal and professional, is presented in this section of the chapter.

5.1.1 Age

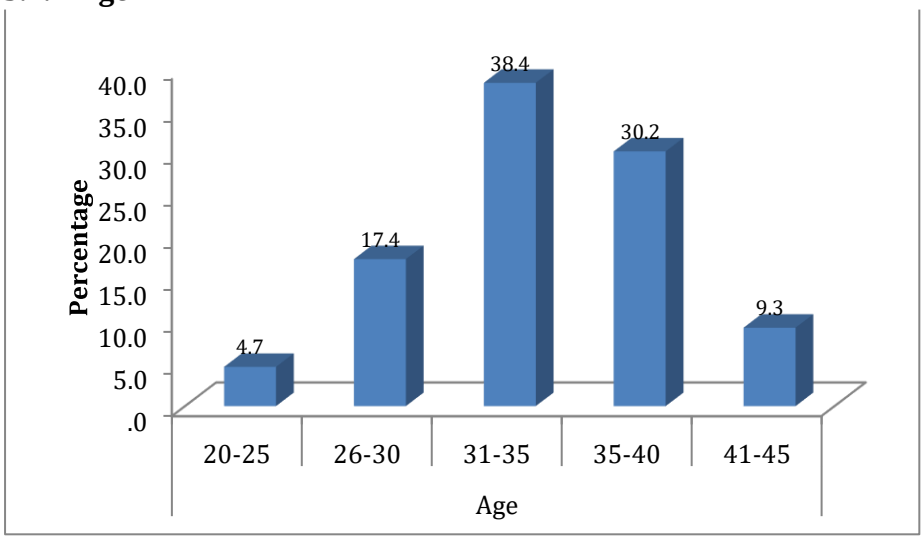


Figure 5.1 Age distribution

As seen in Figure 5.1, the age of the respondents ranged from 20 to 45 years. A total of 33, out of the sample of 86 (38.4%), were aged from 31 to 35, while those aged from 35 to 40 years accounted for

30.2% (26) of the sample. Information technology specialists, in general, must complete a qualification, or develop a skill before they have the competency to assist organisations. This would account for the small number in the 20 to 25 age group.

5.1.2 Gender

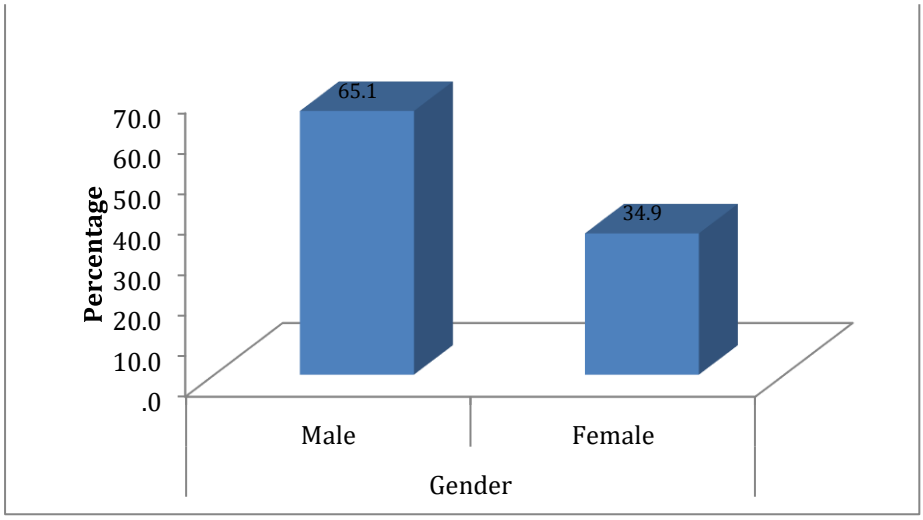


Figure 5.2 Gender distribution

In this study, the majority (56, 65.1%) of the participants are male (Figure 5.2). Information technology is known to be a male dominated space; several attempts have been made to include females, so that they can contribute to this growing sector. The results of this survey are consistent with this trend, with a larger representation of male than female consultants and employees.

5.1.3 Awareness and knowledge about the POPIA legislation

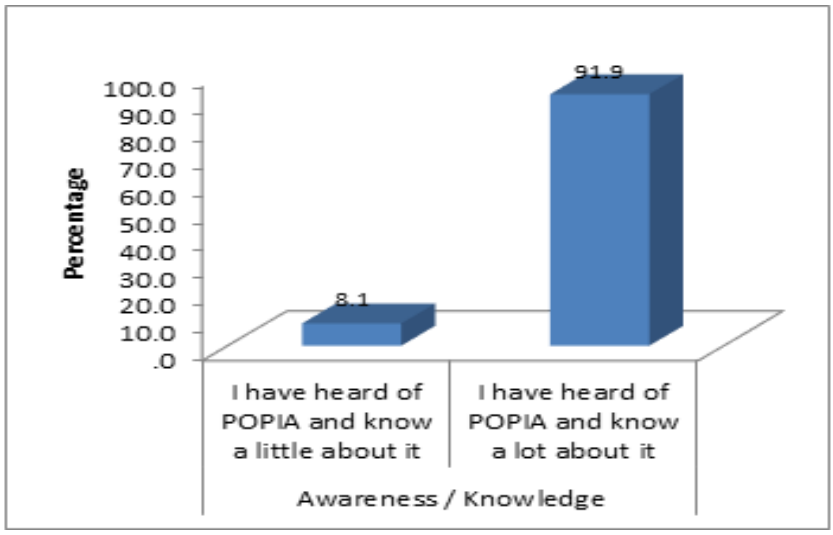


Figure 5.3 Awareness and knowledge about the POPIA

Respondents were asked to rate their level of awareness and knowledge regarding the POPIA legislation. Response options included: I have not heard of the POPIA legislation; I have heard of POPIA but do not know anything about it; I have heard of POPIA and know a little about it; and I have heard of POPIA and know a lot about it.

Results (Figure 5.3) show that all the respondents had heard of POPIA with the majority (91.9%) indicating that they know a lot about it. With most of the participants having a good level of knowledge about POPIA, it increases the chances that they would understand the importance of POPIA and its implementation.

5.1.4 Experience in the field

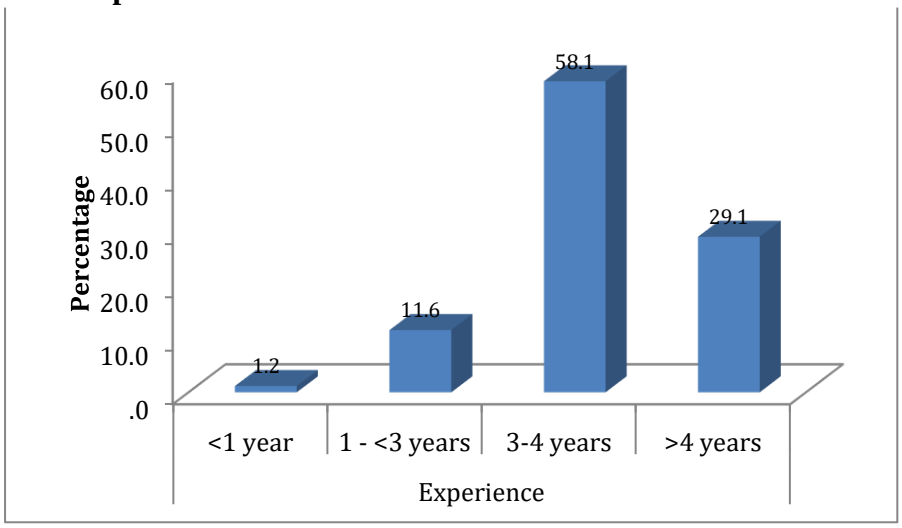


Figure 5.4 Experience in the field

According to Figure 5.4, most of the respondents (50, 58.1%) had 3 - 4 years of working experience in the field, with an additional 25 (29.1%) having more than 4 years working experience in the field. Only one of the respondents had less than a year of work experience in the field. This informs us that most of the respondents have enough work experience to develop systems; will likely be well-skilled and should have a fair understanding of the information security issues affecting IT systems.

5.1.5 Functions performed.

Respondents were asked to indicate which, from a list of four functions, they performed in their organisation. They could select multiple functions, if relevant. The results are summarised in Figure 4.5.

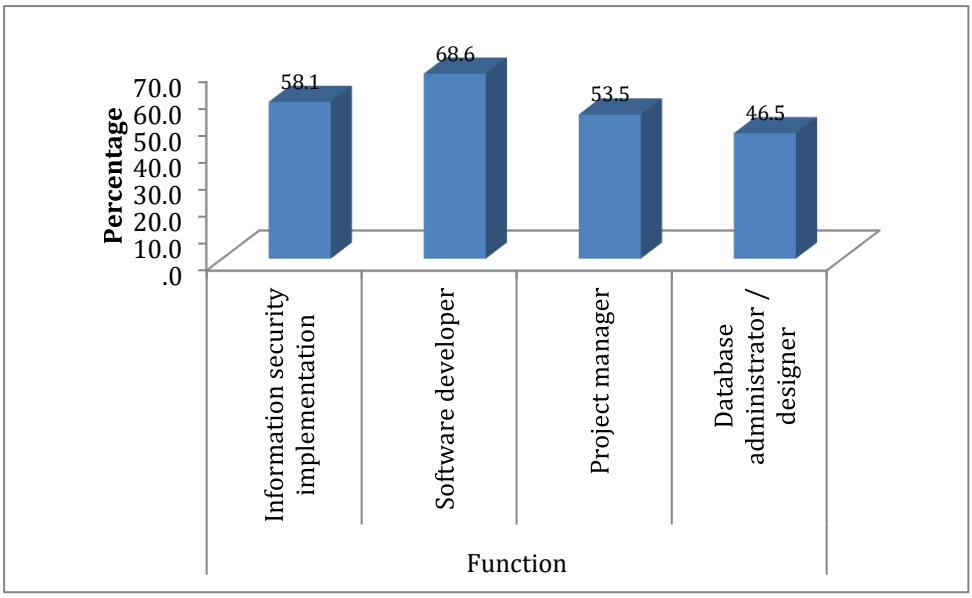


Figure 5.5 Functions performed

It is evident (Figure 5.5) that most of the respondents implement information security and/or develop software and/or manage a project. The function that is performed by the smallest number of respondents (40, 46.5%) is administering or designing databases. We can conclude that most of the respondents perform more than a single function at work. This is because SMEs in general have a lower staff capacity, caused by limited finances; and the majority of them are software developers because the development of SMEs' e-commerce sites is primarily in the hands of software developers. Information security implementation is the second highest as this task is critical in securing information assets belonging to organisations. This shows us that our sample is rich with work experience in various job roles within the IT space. It can be concluded that these respondents fulfil the requirements to participate in the study and know enough about the POPIA legislation to meaningfully contribute to the study.

5.2 Implementing POPIA.

This section of the chapter covers the implementation of the POPIA. Issues such as the best information security frameworks; management support for SMEs to implement the POPIA; risks associated with information security assets within the web-based systems (e-commerce sites); mechanisms used to address information security attacks; the benefits/consequences of POPIA compliance; and organisational and external challenges that affect SMEs when attempting comply with the POPIA legislation are examined. In addition to this, the method of communication used by organisations to inform their customers when confronted with a data breach is explored. Lastly, the method adopted by the SMEs to assess the success rate of their information security training and awareness is reported.

5.2.1 IS best practices and frameworks.

Respondents were asked to indicate which of a list of four frameworks are used in their organisation. The results (Table 5.1) show that most organisations use one or both of COBIT 5 and ISO 27001/27002 when implementing the 7th condition of POPIA. Results from a binomial test show that these results are significant. Significantly few uses GAAP or NIST SP 800 for this purpose.

Table 5.1 Frameworks used.

Item	Frequency (%)		N	p-value
	Yes	No		
COBIT 5	81 (94)	5 (6)	86	<.0005*
IS0 27001 / 27002	81 (94)	5 (6)	86	<.0005*
GAAP	1 (1)	85 (99)	86	<.0005*
NIST SP 800	5 (6)	81 (94)	86	<.0005*

* indicates significance at the 95% level.

5.2.2 Protection of information resources

Respondents were asked to indicate which of four security measures they use to protect the information assets belonging to their organisation. Results from a binomial test (Table 5.2) show that encryption, web application firewalls, and physical security are used by a significant proportion of the respondents. However, database audits are used by only half of the respondents.

Table 5.2 Information security protection

Item	Frequency (%)		n	p-value
	Yes	No		
Encryption	84 (98)	2 (2)	86	<.0005*
Web Application Firewalls	79 (92)	7 (8)	86	<.0005*
Physical Security	69 (80)	17 (20)	86	<.0005*
Database Audits	43 (50)	43(50)	86	1.000

* indicates significance at the 95% level.

5.2.3 Awareness and understanding of POPIA.

Respondents were asked to indicate their level of agreement, on a scale 1 = strongly disagree to 6 = strongly agree to two statements regarding their awareness and understanding of POPIA.

Table 5.3 Opinions on awareness and understanding of POPIA

Item	Responses as Frequency (%)						n	Mean (SD)	t	df	p-value
	Strongly disagree	Disagree	Slightly disagree	Slightly agree	Agree	Strongly agree					
The company provides me with adequate information security training awareness	1 (1.2)	3 (3.5)	9 (10.5)	18 (20.9)	41 (47.7)	14 (16.3)	86	4.59 (1.067)	9.501	85	<.0005*
Top management understands the contents of the POPIA	-	2 (2.3)	10 (11.6)	30 (34.9)	31 (36)	13 (15.1)	86	4.5 (.967)	9.589	85	<.0005*

* indicates significance at the 95% level.

The one sample t-test was applied to test if there is significant agreement or disagreement about management providing adequate information security awareness, and the understanding of top management regarding the POPIA legislation. The average agreement score was tested against the central score of 3.5 Results (Table 5.3) show that there is significant agreement that the company provides adequate information security training. There is also significant agreement that the company understands the contents of the POPIA legislation.

5.2.4 Measure of the effectiveness of POPIA awareness and training tools

Respondents were asked to indicate their use of two information training and awareness methods to measure the success of the information security and awareness training. Results from a binomial test (Table 5.4) show that a significant 76% of organisations adopt questionnaires as their primary assessment tool, but a significant proportion (72%) do not adopt interviews.

Table 5.4 Measure of the effectiveness of training and awareness methods

Item	Frequency (%)		n	p-value
	Yes	No		
Questionnaire	65 (76)	21(24)	86	<.0005*
Interviews	24(28)	62(72)	86	<.0005*

* indicates significance at 76%.

5.2.5 Consent from customers to process data.

When asked if they always get consent from customers to process their data, a significant 80% indicated that they do always get consent before customer data is processed or used by the organisation.

5.2.6 Informing affected customers of a data breach.

Respondents were asked to indicate which of four items (Figure 5.6) is used most often to notify customers when a data breach has occurred. Results from a chi-squared goodness-of-fit analysis show that SMSs/text messages and announcements on the website are the methods adopted significantly more often for communicating data breaches p<.0005.

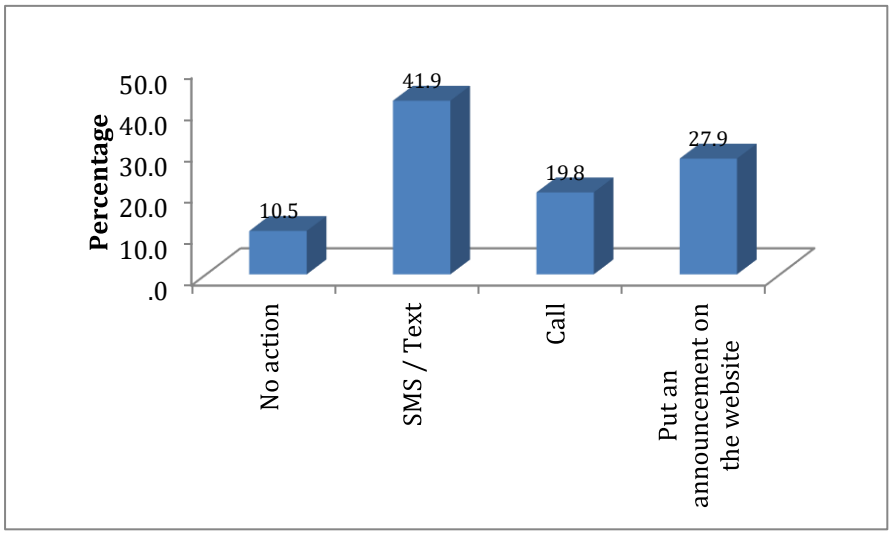


Figure 5.6 Notifications on data breach.

5.2.7 Information security risks encountered.

Respondents were asked to indicate which of three information security threats (Figure 5.7) is encountered most often in their organisations. Analysis shows that there is no significant difference in the incidence of these threats.

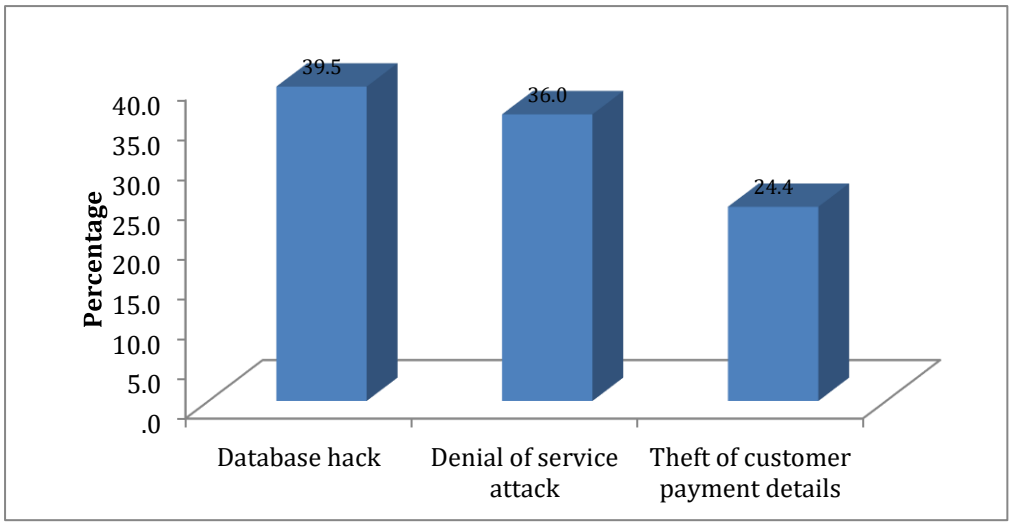


Figure 5.7 IS risks.

5.2.8 Frequency of organisational security risk analysis

Respondents were asked to indicate how frequently they update the risk analysis list in their organisation (Figure 5.8). A significantly small proportion (29 – 33.7%) do this task more frequently than 9 monthly; while a significant 64% update the list at most every 9 months, p<.0005.

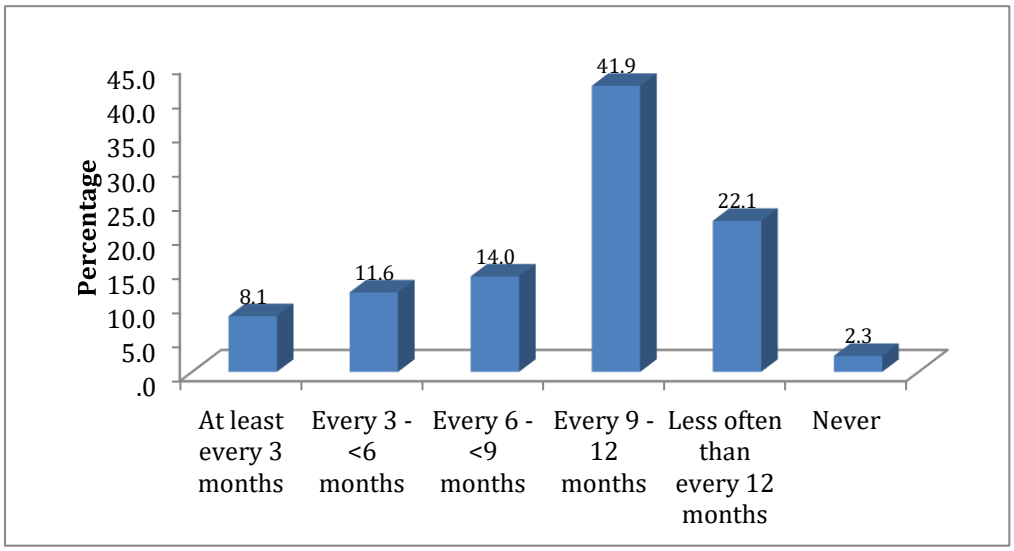


Figure 5.8 Frequency of risks analysis

5.2.9 Management support on POPIA

Respondents were asked to indicate their level of agreement, on the scale 1 = strongly disagree to 6 = strongly agree to seven statements regarding organisational management support on POPIA implementation. Results from a one-sample t-test (Table 5.5) show that there is significant agreement that management provides support to implement POPIA; provides a budget to implement compliance measures; audits the POPIA compliance; ensures that third party organisations are compliant with the

POPIA; provides up to date training to employees so that they know what is right or wrong; and has developed policies to drive POPIA in the organisation However, there is neither significant agreement nor significant disagreement, that management employs an external organisation to oversee certain aspects of the POPIA.

Table 5.5 Management support

Item	Responses as Frequency (%)						n	Mean (SD)	t	df	p-value
	Strongly disagree	Disagree	Slightly disagree	Slightly agree	Agree	Strongly agree					
Management provides adequate support to implement the POPIA 7TH condition	3 (3.5)	4 (4.7)	10 (11.6)	22 (25.6)	34 (39.5)	13 (15.1)	86	4.38 (1.219)	6.722	85	<.0005*
Management provides a budget to implement compliance measures	3 (3.5)	4 (4.7)	9 (10.5)	24 (27.9)	34 (39.5)	12 (14)	86	4.37 (1.198)	6.748	85	<.0005*
Management employs an outside company to oversee certain aspects of the POPIA task	6 (7.0)	11 (12.8)	13 (15.1)	21 (24.4)	26 (30.2)	9 (10.5)	86	3.90 (1.423)	2.577	85	1.000
Management audits our POPIA compliance	3 (3.5)	6 (7.0)	11 (12.8)	23 (26.7)	32 (37.2)	8 (9.3)	86	4.26 (1.248)	5.617	85	<.0005*
Management ensures that third party organisations are also compliant	4 (4.7)	8 (9.3)	16 (18.6)	18 (20.9)	32 (37.2)	8 (9.3)	86	4.05 (1.319)	3.843	85	<.0005*
Management provides us with up-to-date training so that we know what is right or wrong	3 (3.5)	7 (8.1)	10 (11.6)	24 (27.9)	29 (33.7)	13 (15.1)	86	4.26 (1.285)	5.454	85	<.0005*
Management has developed policies to drive the POPIA in the organisation	3 (3.5)	6 (7.0)	11 (12.8)	25 (29.1)	30 (34.9)	11 (12.8)	86	4.23 (1.243)	5.465	85	<.0005*

These seven items are combined to give a single composite measurement (SUPP) for management support. The composite measurement, computed by averaging scores of the individual items, is shown

to be reliable with internal consistency (Cronbach's alpha = .946). Analysis from a one-sample t-test shows that there is significant agreement that overall management support for POPIA exists (Table 5.6).

Table 5.6 Overall management support

Construct	Label	Items	Cronbach's alpha	n	Mean (SD)	t	df	p-value
Management support	SUPP	1 2 3 4 5 6 and 7	.964	86	4.2 (1.112)	5.887	85	<.0005

5.2.10 Consequences of disregarding the POPIA.

Respondents were asked to indicate their agreement that each of four consequences of disregarding POPIA (Figure 5.9) affects their organisations. Results (Table 5.7) show that there is significant agreement that reputational damage; loss of customer damage; heavy fines; and imprisonment are all consequences of disregarding POPIA.

Table 5.7 Consequences of disregarding the POPIA

Item	Responses as Frequency (%)						n	Mean (SD)	t	df	p-value
	Strongly disagree	Disagree	Slightly disagree	Slightly agree	Agree	Strongly agree					
Reputational damage	-	1 (1.2)	2 (2.3)	8 (9.3)	53 (61.6)	22 (25.6)	86	5.08 (.739)	19.843	85	<.0005 *
Imprisonment	1 (1.2)	2 (2.3)	5 (5.8)	11 (12.8)	54 (62.8)	13 (15.1)	86	4.79 (.935)	12.808	85	<.0005 *
Loss of customer confidence	-	-	3 (3.5)	8 (9.3)	45 (52.3)	30 (34.9)	86	5.19 (.744)	21.022	85	<.0005 *
Heavy fines	-	-	3 (3.5)	10 (11.6)	48 (55.8)	25 (29.1)	86	5.10 (.736)	20.216	85	<.0005 *

* indicates significance at 95% level.

5.2.11 Benefits of implementing the POPIA.

Respondents were asked to indicate their level of agreement, on the scale 1 = strongly disagree to 6 = strongly agree to six statements regarding organisational benefits for implementing the POPIA. Results from a one-sample t-test (Table 5.8) show that there is significant agreement that the benefits of implementing POPIA allow the organisations to maintain a good reputation; retain existing/get more

customers; save money from paying non-compliance fines; experience better alignment with existing technology; have better security; and have reduced maintenance costs.

Table 5.8 Benefits of POPIA compliance

Item	Responses as Frequency (%)						n	Mean (SD)	t	df	pvalue
	Strongly disagree	Disagree	Slightly disagree	Slightly agree	Agree	Strongly agree					
Maintain a good reputation	-	-	8 (9.3)	1 (1.2)	55 (64.0)	22 (25.6)	86	5.06 (.802)	18.011	85	<.0005 *
Retain existing / get more customers	-	-	4 (4.7)	12 (14)	50 (58.1)	20 (23.3)	86	5.00 (.751)	18.511	85	<.0005 *
Save money from paying non-compliance fines	-	1 (1.2)	2 (2.3)	9 (10.5)	50 (58.1)	24 (27.9)	86	5.09 (.761)	19.407	85	<.0005 *
Better alignment to existing technology	-	-	2 (2.3)	7 (8.1)	58 (67.4)	19 (22.1)	86	5.09 (.625)	23.618	85	<.0005 *
Better security	-	-	3 (3.5)	5 (5.8)	55 (64)	23 (26.7)	86	5.14 (.671)	22.643	85	<.0005 *
Reduced maintenance cost	1 (1.2)	-	6 (7.0)	5 (5.8)	54 (62.8)	20 (23.3)	86	4.99 (.874)	15.785	85	<.0005 *

* indicates significance at the 95% level.

These six items are combined to give a single composite measurement (BEN) for benefits of POPIA compliance. The composite measurement, computed by averaging scores of the individual items, is shown to be reliable and internally consistent (Cronbach's alpha = .941), Analysis from a one-sample t-test shows that there is significant agreement that, overall, there are benefits of POPIA compliance (Table 5.9).

Table 5.9 Construct of combined benefits

Construct	Label	Items	Cronbach's alpha	n	Mean (SD)	t	df	p-value
Benefits of Compliance	BEN	1 2 3 4 5 and 6	.941	86	5.06 (0.661)	21.922	85	<.0005

5.2.12 Challenges of POPIA implementation

Respondents were asked to indicate their level of agreement, on the scale 1 = strongly disagree to 6 = strongly agree to eight statements regarding challenges experienced when implementing the POPIA. Results from a one-sample t-test (Table 5.12) show that there is significant agreement that challenges of implementing the POPIA include lack of government support to implement the POPIA; dealing with data breaches; getting consent to use data; and adapting to new requirements. However, there is a significant disagreement that the organisations experience the following challenges when implementing the POPIA: lack of support from top management in the form of funding; lack of support from top management in the form of human resources; the POPIA document is not comprehensive and does not provide guidance for implementation; and the organisation does not know where to start when implementing the POPIA.

Table 5.10 Frequency table for management support

Item	Responses as Frequency (%)						n	Mean (SD)	t	df	pvalue
	Strongly disagree	Disagree	Slightly disagree	Slightly agree	Agree	Strongly agree					
Lack of support from top management in the form of funding	13 (15.1)	12 (14)	12 (14)	18 (20.9)	23 (26.7)	8 (9.3)	86	3.58 (1.598)	.472	85	<.0005 *
Lack of support from top management in the form of human resources	11 (12.8)	14 (16.3)	11 (12.8)	21 (24.4)	21 (24.4)	8 (9.3)	86	3.59 (1.552)	.556	85	<.0005 *
The POPIA document is not comprehensive and does not provide guidance for implementation.	12 (14.0)	13 (15.1)	3 (3.5)	15 (17.4)	16 (18.6)	27 (31.4)	86	4.06 (1.837)	2.818	85	<.0005 *
The government does not provide organisations with support to implement the POPIA	3 (3.5)	11 (12.8)	10 (11.6)	9 (10.5)	13 (15.1)	40 (46.5)	86	4.60 (1.618)	6.331	85	<.0005 *
The organisation does not know where to start when implementing the POPIA	15 (17.4)	13 (15.1)	3 (3.5)	7 (8.1)	20 (23.3)	28 (32.6)	86	4.02 (1.946)	2.493	85	<.0005 *

Dealing with data breaches	7 (8.1)	10 (11.6)	5 (5.8)	26 (30.2)	20 (23.3)	18 (20.9)	86	4.12 (1.529)	3.737	85	<.0005*
Getting consent to use data	3 (3.5)	12 (14.0)	7 (8.1)	20 (23.3)	26 (30.2)	18 (20.9)	86	4.26 (1.432)	4.894	85	<.0005*
Adapting to new requirements	8 (9.3)	12 (14.0)	6 (7.0)	26 (30.2)	18 (20.9)	15 (17.4)	86	4.03 (1.583)	31.34	85	<.0005*

* indicates significance at the 95% level.

Factor analysis with promax rotation was applied to explore the structure of these eight items related to challenges. The value for the Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO), of .838, and a significant Bartlett's test indicate successful and reliable factor extraction has taken place. Two factors, accounting for 79.11% of the variance were extracted. The details of these factors are summarised in Table 5.11.

Table 5.11 Organisational and external challenges of POPIA implementation

Construct	Label	Items	Cronbach's alpha - reliability	Variance explained by the sub-construct	KMO
Organisational challenges	ORG	1 2 3 and 5	.941	67.325	.838
External challenges	EXT	4 6 7 and 8	.907	11.783	

The organisational challenges are issues which the organisation has control over; while the external challenges refer to issues which are external to the organisation, which they do not have control over.

Results from a one-sample t-test (Table 5.12) show that there is significant agreement that there are external challenges. However, there is NOT significant agreement/disagreement that there are organisational challenges.

Table 5.12 Organisational and external challenges

Construct	Label	n	Mean (SD)	t	df	p-value
Organisational challenges	ORG	86	3.8 1.603	1.815	85	<.0005*
External challenges	EXT	86	4.3 1.364	5.120	85	<.0005*

* indicates significance at 95% level.

This chapter presents the data chronologically and systematically, based on the items covered by the questionnaire. The objectives and purpose of the study were outlined together. The data collected in this study was analysed using SPSS, which is a computerised data analysis tool. Descriptive statistics showing graphs, percentages, and frequency tables are used to draw a summary of the results. The

literature supported the results where applicable, and such references are cited. The next chapter covers the discussion.

CHAPTER 6: DISCUSSION

This study aimed to produce a frame of reference that can be adopted by SMEs to comply with the 7th condition of the POPIA. In addition to this, to study examined existing data privacy legislation to understand how they are responded to by various information security management systems, and to give an in-depth explanation of information security and its roles in responding to data privacy legislation. Lastly, the researcher collected data from SME IT employees to understand how they implement information security and respond to data privacy legislation. This study is quantitative. It is for this reason a questionnaire was used to elicit data from respondents. This chapter covers the discussion on the data analysis to address the research questions.

The 7th condition in the POPIA legislation relies heavily on the components of information security. The information security elements address issues that seek to safeguard the information assets belonging to an organisation, with the aim of removing security threats. The technical equipment and responsibility for information security is at the heart of information technology practice. Therefore, information security skills and know-how are a key part of IT. As a result, the POPIA 7th condition is a key responsibility of the information technology sector. It was indicated in the literature study that information security management systems are adopted to implement data privacy legislation, such as the GDPR. This agrees with the study results, as ISO 27001 and COBIT 5 were chosen by the respondents as the frameworks and best practices for implementing the POPIA.

The demography of the participants shows that the ICT sector is male dominant, and most ICT practitioners are above the age of 25. This is because the sector requires some form of training which may take up to four years; and most individuals in technical ICT roles are male.

The POPIA awareness among the participants was very high, which is a positive outcome, because organisations need to be informed on the POPIA, so that they can provide the required level of security protocols that align to the POPIA. The participants were strong within the ICT sector because they had a great level of experience working within the sector. This indicates that those who participated in the survey, given that they had been in the ICT industry for a longer period, are informed on the POPIA. Therefore, they know what the POPIA is about. This finding contradicts the consensus in the literature, that organisations do not know about the POPIA. According to the literature, most local organisations are not proactive in implementing data privacy legislation. This is evident from the extensive data breaches that have taken place in several industries. The way the incidents are handled is not in line

with the requirements of the POPIA. Therefore, it seems that organisations are not fully aware. Moreover, international organisations work together in implementing data privacy legislation, such the GDPR. For this reason, data privacy legislation in the European region is proactive.

The ICT sector includes several functions. Most SMEs, due to a lack of resources, utilise their ICT human resources across multiple functions. This enables the ICT professionals to be diverse and perform both technical and non-technical operations; and with that level of experience, they can easily align the POPIA to most ICT functions. This result fits with the existing evidence, as cited in the literature, that smaller organisations do not have the luxury of investing in data privacy legislation; unlike bigger organisations who have the financial muscle. The findings indicate that management supports the organisational needs. However, the government seems to play a less significant role in assisting organisations, thus failing organisations. Therefore, it is imperative for the SMEs to approach the information regulator and seek assistance to implement the legislation. Likewise, it is imperative for the information regulator to assist organisations at all levels with compliance. While the literature informed us that POPIA compliance does not discriminate against organisations based on size and financial resources, it requires all existing organisations to be compliant. Therefore, the findings show that SMEs are also working towards aligning with the POPIA legislation.

There are multiple best practices and frameworks that are adopted to implement data privacy regulations, globally. As confirmed by the respondents, the most acceptable framework and best practice for the POPIA is COBIT 5 on information security, and the ISO 27001/27002. This is because they provide a more robust implementation guidance and can be adopted in conjunction, to speak directly to the needs of the POPIA legislation. As the literature pointed out, GDPR requirements are satisfied by the ISO 27001/27002. While other frameworks are available, they are found to be less attractive because of their manual and convoluted processes, which may require more resources for implementation. Therefore, COBIT 5 and ISO 27001/ 27002 can be combined to develop a strong framework for implementing the 7th condition of the POPIA. E-commerce systems are prone to multiple threats as data transits on the internet. Furthermore, the internet has become a focal point for businesses to reach customers and make business transactions. The literature shows that mobile devices are used for shopping on e-commerce sites. The POPIA now sits on the foundation of IT systems. Therefore, it is imperative for security frameworks and international standards to be adopted as part of an organisation’s information security management system.

There are various information security protection mechanisms that affect organisations. However, for this research, only a few were selected because of their prominence in web-based systems. These are encryption, web application firewalls, physical security, and database audits. The information gathered from the participants indicates that most of the organisations they work for employ these mechanisms

to safeguard their information security assets. As seen in the literature, most security threats are usually solved through the adoption of the mechanisms indicated above. This is a positive outcome as most of the POPIA requirements require that the organisations adopt these mechanisms for compliance.
However, one of the mechanisms is not employed or recognised in full. This is the database audit process. This process is key in ensuring the data integrity of records stored. If such a process is not fully adopted, the organisation might not be aware of certain security-related flaws which may affect the data integrity while data is in storage. This process needs to be covered in full. Most organisations cited in the literature adopt this process to satisfy data privacy requirements. Furthermore, the literature also informed us that, for organisations to trade internationally, they need to fulfil common information security practices. Therefore, all processes and steps must be practised. If database audits fulfil the GDPR requirements, then those who are affected by the POPIA, and need to trade within the European market, must perform database audits.

The literature review showed that data privacy legislation is often neglected, especially when it comes to implementation. This is in complete contradiction with the results of this study, which prove that there is an effort from SMEs in the e-commerce sector to align to data privacy legislation. Furthermore, management in the organisations are working towards an alignment with the POPIA by supporting its implementation with training. The SMEs in general have strict budgets for initiatives that do not directly generate returns. As is reflected in the literature, implementing a complete information security management system requires a reasonable budget. The budget is required to purchase hardware and software components to invest in information security, and subsequently implement the POPIA. Results show that SMEs, because of their size and limited resources, utilise their IT resources across various functions, with the aim of developing the e-commerce site and fulfilling the requirements of the data privacy legislation. However, they stretch their resources and work towards compliance.

The literature review indicated that consumers are also responsible for protecting their own information and data privacy. It is for this reason that organisations need to provide their consumers with information they can use to identity and deter suspicious activity on their accounts, as well as knowing the importance of protecting their secret information. The findings of this study have shown that most of the SMEs do not have adequate resources to empower the customers with such information. Lastly, there are multiple approaches that can be adopted to educate consumers, including, but not limited to, a webpage warning the users of threats and vulnerabilities.

In the literature review it is stated that some international web-based organisations adopt various ways to inform customers how their data will be used. Some put up a notice on the top bar of a site, while others put this notice on the e-commerce site's user registration page, thus making it mandatory for a user to agree to any terms and data privacy policies before proceeding with any data exchange on the

online system. The results have shown us that not all organisations ask for informed consent, which is one of the key requirements indicated in the POPIA. Furthermore, the literature shows us that certain organisations do not explicitly state their terms and conditions and omit sharing important information with the consumers. Therefore, they are at risk of non-compliance with data privacy regulations, as the user must consent to every action that will be taken against their data. Lastly, organisations who do not fully adhere to this are not compliant, and the POPIA legislation does not offer partial compliance.

The literature further indicates that businesses who trade internationally need to do so with countries or organisations that follow a similar data privacy as they do. The same applies with the POPIA. Therefore, when SMEs in South Africa do business-to-business transactions with any country outside of South Africa, through transactions that expose South African-based customer data to any external third-party organisation, they must ensure that the third-party organisation, or the international company, adheres to a similar legislation to the POPIA. This broadens the issue of cross-border compliance. The findings show that certain SMEs who do not comply with the regulations will be affected, even when they are protecting their data within the consent clause. This shows that compliance with the data legislation is not only for customer-to-business transactions, but also involve businesses and the international market.

According to the literature, an organisation does not give customers the option to consent to how their data will be used, but have stringent data security measures on their systems, are still not compliant. The findings show us that some SMEs conduct their risk assessment regularly and have strong data protection mechanisms. However, they do not get their users' consent. Such organisations are not compliant with the legislation and will be affected by repercussions that affect the non-compliant. Compliance with the POPIA requires a holistic POPIA approach from the organisation to succeed with implementation.

Based on the literature review, there has been an increase in online transactions, and most transactions happen on the internet. Furthermore, organisations in South African have been hit by an increasing number of cyber-attacks on the internet. In addition to this, smaller organisations are known to be weak because they do not have enough resources to deter newly-introduced threats. As a result, SMEs have been chosen as the main targets. The results of this study also suggest that SMEs do not have enough resources to execute complete and proactive information security. Most of the SMEs utilise the same IT consultant across various IT functions. Internet-based threats have the potential to put SMEs offline, as they may be hit by denial-of-service attacks, or ransomwares. It is for this reason that SMEs must treat the POPIA not as just legislation, but also as a core business strategy.

Security training and awareness programmes offer organisations a human-based firewall. The staff members that are informed are a great investment, like a tight data privacy system. This is one of the

key fundamentals that are covered in the literature review. The results show us that SMEs have a good information security awareness training process which is backed by management support. This finding agrees with literature.

As organisation upgrade their systems, they find themselves being challenged by new types of threats. In addition to this, intruders find new methods to infiltrate technological systems, as indicated in the literature. When organisations migrate to cloud-based services, it assists them to reach their business objectives, but they still inherit the data security vulnerability that comes with the systems. The organisations need assistance from capable IT security individuals to avoid such security vulnerabilities. The findings shows that most SMEs do not have a proactive approach to guarding against newly introduced threats, and the majority do not conduct timeous assessments. This finding proves that the organisations need to have a proactive approach to information security.

The literature informs us that there are numerous cybersecurity-related attacks that go unreported. This is because the POPIA legislation is not yet fully implemented. Furthermore, the POPIA legislation states that organisations have to share data-related breaches with the public, which could cost them their good reputations. Results show that most organisations do know about the POPIA, but do not have the technical skills to deter the threats. Therefore, organisations will be forced to align with the POPIA to protect their reputations and avoid being reported to the information regulator, who oversees POPIArelated complaints from the public and third-party partners.

As stated in the literature review, when systems operate online, organisations only have to update a website. However, when they develop a mobile application for the market, they have an extended responsibility to develop security patches that will ensure a safe information security environment. POPIA regulations are not limited to online sites, but to the whole computing environment for organisations that operate server-side systems. Therefore, an SME that decides to extend their ecommerce services to the market through a mobile application must adopt the same principles for data security on both their web and mobile platforms. Data privacy and security is not only limited to websites. What makes mobile applications more sensitive is their need for regular updates to improve security features, among other features relating to the business. When SMEs rarely conduct a risk assessment, it means they are unable to perform any threat-related patch on their system. In the event they plan to release a mobile application, they will have an extra layer of security vulnerability. The risk assessment component is fundamental in the POPIA. The results show that organisations are poor at this and will be found to be non-compliant and in breach of the POPIA legislation if assessed, or have a security-related case with the information regulator.

The literature shows that organisations do not find themselves in a space to have their POPIA maturity levels measured. The maturity levels are of great concern as they indicate the strength of the efforts made by organisations when implementing the POPIA. The results should be considered; especially where organisations fail to complete a frequent risk analysis and use their independent know-how to implement the 7th condition of the POPIA. The results show that organisations are not proactive in their risk analysis. This opens doors to many threats that may affect the organisation.

Management in an organisation makes a financial commitment to ensure that an information security training and awareness programme is provided to its employees. The aim of such security and awareness training is to ensure that the staff is trained on information security issues. However, the effectiveness of the training must be assessed. Therefore, the organisation must employ a method to measure the effectiveness. The well-known assessment methods are either questionnaires or interviews. Most of the respondents informed us those questionnaires are employed to measure the effectiveness of their security training and awareness. This is a positive outcome, as employers can provide the required remedial training to cover issues needing attention which are picked during the assessments. As indicated in the literature review, information security, which is the foundation for satisfying the 7th condition of the POPIA, requires an investment to comply with the legislation. Such an investment would be to hire the required skills sets, and obtain the resources to safeguard information assets. These resources are physical and logical (hardware and software). Furthermore, the 7th condition of the POPIA states that employees who operate external persons' data must be competent. This means that organisations must appoint a person and ensure that they are competent to operate the data. Lastly, as confirmed by the literature review, information security requires an effort from the organisation.
Therefore, the human resource of the organisation must be competent.

The POPIA 7th condition clearly specifies that an individual must be informed about how their data is going to be processed. Furthermore, it is vital for the individual to consent to how their data will be processed. The respondents are in full alignment with this process as the vast majority agreed to have compliance with the informed consent clause. These respondents have clearly indicated that this process is satisfied, as it is key to aligning with the POPIA legislation. The results show that organisations do explain the terms and use policy for data, to the users, prior to collecting and using the data. This is vital. This initiative speaks directly to the informed consent requirements in the 7th condition of POPIA. Furthermore, the literature reiterates that it is imperative that data subjects are informed about how their data is processed.

When a data breach takes place, the 7th condition in the POPIA legislation stipulates that the affected individuals must be informed. The method of communicating such messages can vary, based on an organisation’s preference, but must be either placing an announcement on their site, texting the affected

persons, or through mainstream media. Respondents have made it clear that they inform their customers when a data breach becomes apparent to them. This is an excellent POPIA practice, as affected parties must be notified when their data is affected, and the organisation should also outline the remedies adopted to prevent further damage. The fastest method of delivering information to many people is through text messages. Therefore, the organisations have adopted an efficient method of delivery. Once customers are notified, they may use the information to address further potential harm. As confirmed by the literature, and prevalent in most information security practices, an affected individual who is informed of a data breach is able to take the necessary steps to ensure that they are not affected any further. This reduces the risk of further damage.

The literature shows that information security risks vary and affect organisations in different ways. In addition to this, they may affect the full operation of an organisation. Therefore, it is vital for an organisation to secure its information assets from such attacks. The attacks are, but are not limited to, database hacking, denial-of-service attacks, and the theft of customer payment details. These issues may affect the organisation in various ways, but also have an impact on the individuals whose data is affected. Respondents have stated that these security risks affect them. Such threats affect business continuity, and it is vital for them to be limited. When card details are stolen, intruders can make illegal transactions, thereby affecting the individual whose card details are stolen. The card details are entered by e-commerce customers when paying for an item. As indicated in the literature study, a database hack, by its nature, exposes the data contained in a database to intruders. The data could be personal information of customers, including payment data, if kept in the database. A series of attacks can render the systems of an organisation unavailable. These attacks affect the business continuity and it may require significant financial resources to limit them. Therefore, it is paramount for data to be safeguarded. Furthermore, it is indicated in the literature that data security issues arise because of such attacks. Therefore, these issues must be addressed by borrowing solutions from information security management systems and complying with data privacy legislation. This finding agrees with the literature review.

Security risks may affect an organisation at any time. The risks vary, and new risks can be introduced at any time. The literature informs us that security risks are introduced by intruders who seek to find ways to steal data or disrupt services of an e-commerce site. The respondents have indicated a lack of proper risk assessment, as they do not frequently do risk assessments. Furthermore, the literature informs us that organisations who fall behind in risk assessment will not be able to deter newly introduced risks which may affect the organisation. Therefore, the respondent's organisations are not proactive, and are vulnerable to newly-introduced risks. The POPIA, in the 7th condition, makes it mandatory for organisations to invest in investigating new risks. This encourages proactive information security as it enables the organisation to find ways to deflect the risks before they become an attack.

The literature review indicates mechanisms that can be adopted to deter risks. These mechanisms are born from risks and attacks. Such risks may affect business continuity or lead an organisation into a situation where they are in breach of data privacy legislation. Therefore, it is important that organisations invest in information security management systems, as mentioned in the literature review.

The POPIA document indicates that management in organisations must support the implementation of the POPIA. The POPIA, in organisations, is driven by management. Respondents have indicated that they receive assistance from management. This is a key requirement when any POPIA-related matter is considered. Organisations must develop a policy to ensure that they cover the POPIA regulations internally. Such a policy will assist in driving compliance. As indicated in the literature review, top management drive policy development and information security implementation. Furthermore, the POPIA legislation makes it a requirement for top management in organisations to allocate a competent person who drives the POPIA implementation.

The POPIA document indicates that an organisation that does not comply with the legislation will be liable to either financial censure or imprisonment. The respondents have indicated that they are familiar with the drawbacks of non-compliance with the POPIA, but were not fully aware that imprisonment is a potential consequence. The literature also shows that organisations are not fully aware, especially about the nature of the incidents that take place. Therefore, this finding agrees with the literature. This finding demonstrates that the organisations may lack adequate knowledge of the POPIA, as imprisonment is one of the extreme punishments they should seek to avoid. It is for this reason that a frame of reference is paramount. Organisations use their own knowledge when approaching the POPIA. Such knowledge may not be adequate for the needs of the legislation. As a result, the organisations pay the price for non-compliance because of external issues which they have no control over. The literature informs us those international organisations rely heavily on the guide provided by their legislative bodies; while South African-based organisations rely on their own understanding.

The literature indicates that the information regulator has not acted on numerous cases opened against businesses who were in breach of the data privacy legislation. This suggests that the IR is not putting much effort into holding non-compliant organisations to account. As a result, SMEs and other businesses have not seen the IR in action, and there is limited knowledge in SMEs regarding the repercussions of POPIA non-compliance. The finding has shown that external organisations are the ones that have not put an effort into implementing the POPIA.

There are various benefits of POPIA implementation. Such benefits are important and are an investment into organisations. Furthermore, the benefits provide organisations with the ability to secure their reputations. The respondents indicated that they are fully aware of the benefits. The benefits should be

one of the key indicators that organisations adopt the POPIA legislation. The respondents have indicated a strong knowledge of the benefits obtained through POPIA compliance. However, this finding is in contradiction with literature, which states that organisations are not compliant because they are not familiar with the benefits thereof. Therefore, this finding disagrees with the literature.

Every legislation in place has its implementation challenges. Such challenges may be internal or external. Internal challenges are organisational management and human resources, as well as finances. There are also external challenges. Such challenges are, but are not limited to, governmental support, the POPIA document guideline, and how to deal with data breaches. The respondents have indicated that they have no internal challenges, but that they have vast external challenges. This means that external challenges are hindering the organisations in implementing the POPIA. The government, as the regulator and the state organ that oversees and promotes the POPIA, has not been able to provide SMEs with the relevant resources required to comply with the legislation. This is a key drawback for implementation, as the government must play a role in ensuring that it provide any organisation with clear implementation guidance which can assist with compliance. As a result, it is the external challenges which directly reflect the efforts of the government regarding POPIA implementation. Therefore, it is vital that the government supports organisations with a POPIA compliance guide. Furthermore, this means that the efforts made by organisations when aligning to POPIA are based on their independent views of what is correct or incorrect. The literature indicates that organisations must adhere to the guidelines of the data privacy legislation as they are. The finding proves that organisations are not fully adhering with the POPIA document because its 7th condition is incomplete. Therefore, the efforts by organisations might not be sufficient, and organisations may be investing in something which does not meet government requirements.

Employees in different functions of the POPIA implement the POPIA using internal knowledge based on existing information security management systems. None of the organisations are fully reliant on the government's POPIA document, as it is a legal document that does not provide a guide for implementation. There is little engagement from the government with entities regarding the POPIA initiative. However, organisations have found themselves in a position where they needed to develop an internal guide. The drawback of implementing the POPIA without using an external guide developed by government is that compliance cannot be fully achieved, and organisations end up doing what they think is good enough for compliance. This may cause them to miss important aspects and suffer noncompliance. The literature has indicated the cost of non-compliance, showing that reputational damage, imprisonment, and financial fines are among the repercussions that affect organisations. In addition to this, organisations will not realise the benefits of the POPIA as they may not satisfy the POPIA, as the POPIA 7th condition is not an adequate guide towards compliance. For this reason, this research aims to deliver a frame of reference for the 7th condition of the POPIA.

As mentioned in the literature review, the organisation that does not invest in its information security has a greater risk of exposing its customers' data to intruders. As a result, the customers' data is compromised, and further damages can occur. For example, an organisation's data can lose its data integrity. Therefore, it is paramount for organisations to safeguard the information belonging to its customers. The financial investment required could be used to train staff, and procure software and hardware equipment to reduce information security threats. E-commerce systems are affected and should be protected by SMEs. As confirmed by the literature review, South Africans shop online. Therefore, SMEs who operate their online stores must adopt the POPIA to safeguard the data integrity of customers and ensure that they operate within the boundaries of the POPIA. The quality of information security systems employed to safeguard data is determined by the financial investment made by the organisation.

The literature has discussed the various incidents that affect e-commerce sites, such as spamming; hacking; various tools and methods used for spoofing; injecting malicious software; and denial-ofservices attacks. To reduce the risk from these incidents, organisations require information security mechanisms. These mechanisms are information security management systems, used to protect organisations' information resources and maintain the data integrity. The management of organisations, as mentioned in the literature review, needs to play a large role in developing internal IT policies that ensure that data privacy regulations are adhered to. The literature study confirmed that, in the context of increasing levels of attacker sophistication in the connected world, massive data breaches occur from e-commerce system transactions. The findings show us that SMEs are not proactive and fail to do risk analysis to deter new, sophisticated risks. Therefore, they run the risk of being affected by security breaches.

The GDPR, as mentioned in the literature review, was used to develop the POPIA. Various organisations within the European region use ISO 27001/ 27002 as a frame of reference to implement GDPR. Therefore, parts of the 7th condition of the POPIA can be successfully addressed through a framework such as the ISO 27001/27002. However, findings show that an additional framework, such as the COBIT 5, can be used in conjunction with the ISO to develop a stronger frame of reference to assist in the implementation of the 7th condition of the POPIA in full. The POPIA document, in the 7th condition, specifies that organisations must look for tools and frameworks to assist them to implement the POPIA. In addition to this, more than one framework can be used to address different components of the data privacy legislation. Findings in this study indicate that ISO 27001/ 27002 is a stronger information security standard adopted into information security management systems, to safeguard their information assets and respond to data privacy regulations. The findings agree with the literature, that an information security management system is key in servicing the information security needs of organisations. For

this reason, ISO 27001/ 27002 has been used internationally to secure the data integrity and confidentiality of an organisation. As cited in the literature, GDPR implementers adopt ISO 27001/ 27002. Therefore, ISO 27001/27002 would be valuable when implementing the POPIA.

The literature states that organisations trade globally, and the process of trading might be restricted by the data privacy legislation in different continents and countries. Therefore, for South African businesses to trade successfully at a global level, they may be required to be compliant with existing international data privacy legislation. For any non-European business to service European customers, they need to be GDPR compliant. This means that a business that does not implement GDPR is affected. Therefore, it is paramount that South African businesses of all sizes find a way to be compliant with POPIA. Data privacy regulations are taken seriously in first world countries. The literature review has provided us with evidence that South African organisations in general are lax with implementing the POPIA. The results of the study are in full agreement with this. There are various data breaches that have occurred in small- and large-scale organisations. The same security challenges affecting largescale organisations are inherent in smaller organisations. The primary issue highlighted in the results is that government intervention is not adequate to assist organisations with implementation. Therefore, organisations need a frame of reference that can be adopted to implement the POPIA.

There are various information security management systems. These systems cannot comply with the POPIA without detailed specifications of what the POPIA requires in the 7th condition. It is not useful for organisations to assume they understand the requirements of the 7th condition of the POPIA in order to implement it. This does not solve the compliance challenges, but provides the organisation with more administrative work. The literature informs us that advocate Pansy Tlakula is the information regulator. As the information regulator, her office is there to oversee and manage POPIA issues affecting South Africa. In addition to this, the IR is the office which needs to assist organisations with POPIA by developing tools and guidelines. It has been indicated in the findings that the IR does not provide the required level of support to assist SMEs with understanding and implementing the POPIA, and SMEs are left with the task of implementing their own understanding of the regulations. In addition, the IR's office is currently short-staffed and does not have the capacity to address all the POPIA requirements of organisations. The literature has informed us that only key roles were filled, and there are still numerous vacancies in the IR's office. This is one of the external challenges mentioned in the findings.

Non-compliance with the POPIA can be punished by imprisonment and fines, just like other international data privacy legislation. The organisations also stand a great risk of losing customer confidence and closing. These repercussions are experienced by those in the European region, the United Kingdom and Asia when they fail to adapt to their data privacy legislation. The literature confirms that organisations are likely to be penalised when they violate the legislation. The 7th condition

of the POPIA needs to be presented within a framework that can assist organisations with a roadmap to towards implementation.

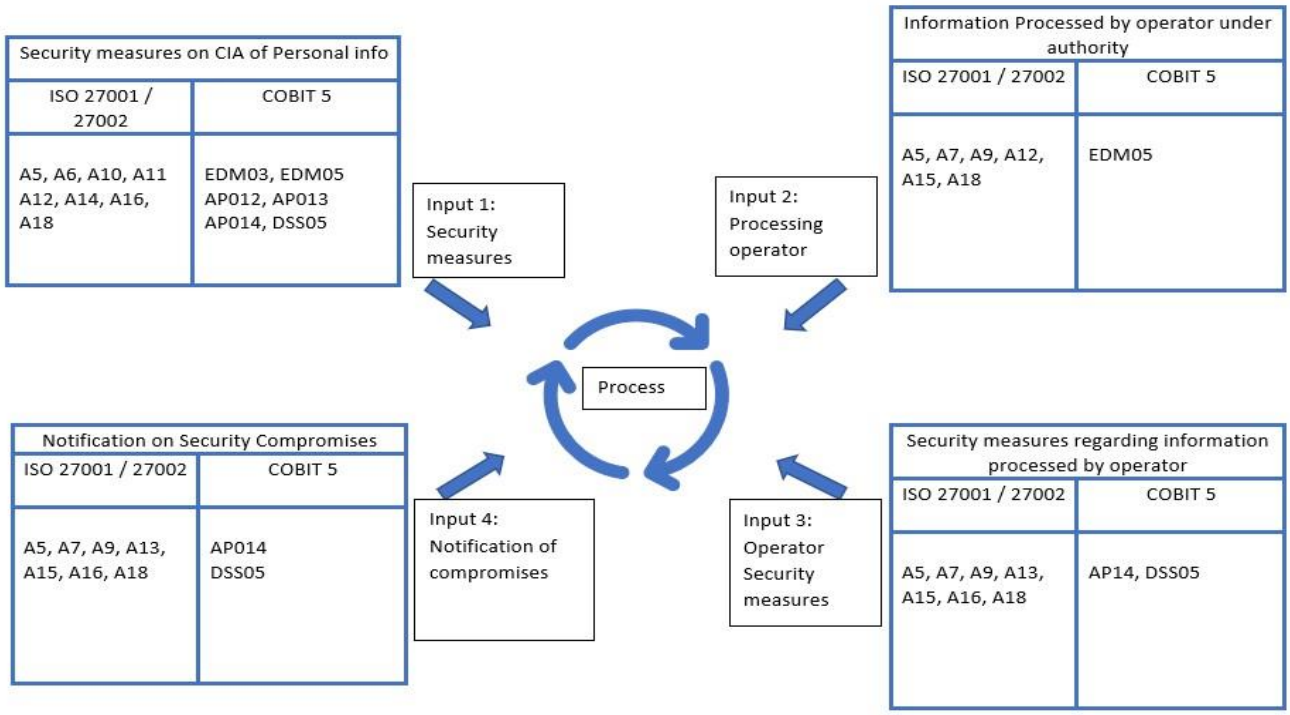
Security breaches that affect organisations reveal loopholes in the organisation's information security management systems. The literature informs us that, if an organisation stores encrypted data in their databases, this makes the data unreadable, even if it is accessed by intruders. However, if an organisation uses an encryption standard that can be easily bypassed, it does not provide any security to the data stored if it is hacked. This also affects other information security mechanisms such as web application firewalls, physical security, and database audits. As stated in the 7th condition of the POPIA, it is vital for an organisation investigate newly introduced threats constantly, to understand the best way to safeguard its information resource. The literature review has indicated that, in the GDPR, a risk analysis is carried out extensively and proactively by affected organisations in response to the legislation. The findings in this study contradicted the literature, as most of the organisations did not conduct frequent risk analyses. These risk analysis strategies are important for organisations to understand and implement the POPIA legislation.

The framework developed in this study in its entirety is based on the contribution of the participants, existing Information Security international standards such as COBI 5 for information security, ISO 27001/27002, and existing literature which directly speaks to GDPR. In addition to this, the researcher consulted the POPIA processes which are reflected in condition 7, and these sub processes are mentioned in chapter 7 under input 1,2,3, and 4 respectively. These sub processes were dissected and aligned to processes that address them in COBIT 5 and ISO. Both COBIT 5 and ISO were selected by the participants as they address most concerns in information security management systems.

CHAPTER 7: FRAMEWORK

This chapter presents the framework developed in this study. As already indicated, the researcher adopted the views of the participants, literature, and existing professional bodies in information security and developed this framework. In addition to this, the four items named (item 1, item 2, item 3, and item 4) are the four pillars in the 7th condition of the POPIA. The four pillars are aligned to processes found in COBIT 5, and ISO 27001 and 27002.

7.1 Framework for the 7th condition of the POPIA



The respondents indicated that COBIT 5 and IS0 27001/ 27002 are best suited for POPIA compliance. It is also evident in the literature that ISO 27001/ 27002 is highly regarded for implementing information security management systems and responding to data privacy legislation such as the GDPR. It is for this reason that the researcher developed a frame of reference using the ISO 27001/ 27002 and COBIT 5. This is a high-level framework which can only be applied to the SME e-commerce sector.

7.1.1 Input 1

In this process, a responsible individual within the organisation must be selected to make sure that the organisation's data, systems, and processes have integrity, and data belonging to customers are treated

with confidentiality. The necessary technical measures must be put in place. This involves the necessary hardware and software components. In this step, the security mechanisms employed must manage the organisation's internal data policy. These mechanisms would ensure data integrity. The columns showing ISO 27001/27002 and COBIT 5 indicate the components in the best practices that speak to data integrity and confidentiality. These are in line with the POPIA 7th condition.

7.1.2 Input 2

In this process, the data operator, acting on behalf of the organisation, must process the subjects' data according to the informed consent that was sent to the subject. In addition, the data processed must not be exposed to anyone who does not fit into the consent acknowledged by the data subject who owns the data.

7.1.3 Input 3

In this process, data access levels, non-disclosure agreements, and confidentiality clauses play a role. Furthermore, technical measures ensure that a user has the security authorisation required to access data, and to conduct the operation within limited boundaries to ensure that the organisation has appointed only responsible and informed individuals to operate the data. In addition, users or data subjects must be informed of the operations that will be performed on their data. Lastly, the individual appointed must, in the event they suspect a data breach, report such to the relevant person in the organisation. In COBIT 5 and ISO 27001/27002 columns indicate the processes from the best practices and framework, to deliver this process.

7.1.4 Input 4

In this process, the COBIT 5 and ISO 27001/27002 components ensure that organisations are responsible for informing affected people when their data is compromised. The information must be given to the customers as soon as the organisation becomes aware of a breach. In addition, the organisation must ensure that the relevant law enforcement bodies are informed. Lastly, the notification must explicitly and precisely indicate what happened, how the organisation plans to resolve the issue, and the possible consequences of the data compromise.

7.1.5 Process

The process step, which is in the centre of the framework, is there is show that all four inputs must be connected. The reason for the connection is to ensure that the four process are joined together so organisations can meet the requirements of compliance with the 7th condition of the POPIA's technical measures.

CHAPTER 8: CONCLUSION, AND RECOMMENDATIONS

8.1 Conclusion

The study covered four major questions and delivers a single framework for SMEs to use as guide when implementing the 7th condition of the POPIA. A theoretical and conceptual framework was used to guide the development of the framework developed in the study. Information security components were also introduced in managing the processes and matters relating to the POPIA. The main objectives were to understand the impact of information systems on the POPIA; to understand how employees in different functions of ICT in the SMEs implement the POPIA; and to examine the challenges, benefits, and disadvantages related to POPIA implementation.

The POPIA is legal legislation that has eight conditions. The 7th condition in the POPIA, which covers security safeguards, is written in a legal manner, but requires technical measures from information systems. Information systems processes, including the CIA (confidentiality, integrity, availability) are components the 7th POPIA condition requires. Therefore, there is a closely aligned relationship between the CIA triangle of information security and the requirements indicated in the 7th condition of the POPIA. The information security field itself is rich in technical measures and know-how to address the conditions of the POPIA. Therefore, the POPIA relies heavily on information security. RQ1

SMEs have employed their ICT consultants for various functions. These roles include software development; information security; databases; and project management. The SME ICT personnel who fulfil these functions have displayed a fair understanding of what the POPIA entails. However, they have indicated that they rely on their own understanding of the 7th condition of the POPIA and adopt various information security processes to satisfy the requirements indicated in the 7th condition of the POPIA, since the 7th condition requires technical knowledge. In addition, the SME personnel indicated that management provides them with support, finances, and training. However, they are unable to determine if they are aligned to the correct processes, as the POPIA requires technical measures, yet it is written in a limited and legal manner. The SMEs have been doing what they think is best suited to cover the POPIA. In some processes they display little or no understanding of what they should do, specifically in the 7th condition of the POPIA. Therefore, a frame of reference would be invaluable in assisting the technical teams in organisations to build systems which are properly aligned to the POPIA. RQ2

The SMEs have indicated that their biggest challenge is understanding what the legal POPIA document requires of them, as far as the 7th condition of the POPIA is concerned. In addition to this, it has been shown that they have external challenges in implementing the POPIA, in general. External refers to government support and the POPIA document. Therefore, the main challenges for them are to

understand what the POPIA document requires, preferably through a framework, to align with the POPIA. In addition, government should have a unit to assist with POPIA implementation, and not only an office for reporting security breaches. Some organisations have internal challenges. These are closely related to a lack of management support and the budget comply with data privacy legislation. An organisation that is found to be in breach of the POPIA, will be sanctioned with fines, imprisonment, and, most of all, a damaged reputation. RQ3

There are many benefits an organisation enjoys from being compliant with the POPIA. These benefits enable to the SMEs to maintain a healthy business reputation; increase customer loyalty and satisfaction; have a better alignment with existing technology; maintain better system security; and save money by not having to pay non-compliance fines.

The POPIA legislation indicates that organisations that are found to be in breach will be liable to a fine or imprisonment. However, organisations suffer more by seeing their reputations damaged and losing customer confidence, which drives sales down. The legal repercussions are costly, but the ones that affect customer loyalty have the greatest impact on the organisation's sales and operations. An organisation that can afford to pay the legal fine for non-compliance, will need more than the legal fine to retain its customer confidence. RQ4

8.2 Limitations of the study

The results of the study are limited to the e-commerce IT sector for SMEs, and the area in which the study was conducted. Furthermore, it is important to note that this is a high-level framework and cannot work to resolve the POPIA issues in all industries. Bigger organisations may need to expand on the framework for it to fit their needs.

8.3 Recommendations

From the findings of the study, the following recommendations have been made in connection with information security practices, and POPIA in SMEs.

1 It is imperative that organisations consult with the Information Regulator for help guides and context to the POPIA regulation in general. The context in which the regulation is presented is legal and generic. However, the repercussions are explicitly direct. Therefore, the IR needs to have a department that seeks to find ways to assist SMEs with fulfilling the legal requirements. This is because the findings show that SMEs have internal measures to implement the regulation. However, they are defeated by the external measures, which is governments involvement in this newly enforced regulation.

2. A common trend within the findings showed that organisations from top to bottom level of management show interest with the POPIA and find ways to implement its requirements. However, they made it evident that they are implementing this regulation and its requirements based on their own understanding. Thus, they are not sure if the effort they put in covers the requirements of the regulation. This means that organisations are not sure if they are meeting the requirements of the regulation, even when they put the efforts required to implement it. It is recommended that organisations must not depend on their own understanding as they might lose a significant number of resources, such as time and money. Therefore, they must not implement what they are not sure about.

3. The existing best practices and frameworks which are developed , have a good reputation in tackling data privacy regulations and information security in general, can be used as an ingredient for implementation some of the components identified in their POPIA such as the issue of consent or encryption as an example. Such best practices can be adopted proactively.

4. It is vital for organisations at all levels, including management, to invest in the implementation of the data privacy legislation. This investment would bring a return on investment to the organisation as it will safeguard its reputation. It is seen in literature that the biggest loss to an organisation besides imprisonment, and financial fines, is reputation. Once an organisation loses its reputation, they lose their most valuable asset. Therefore, an investment towards the POPIA itself will keep the organisations data privacy related affairs in a better position.

5. The findings proved to us that most organisations do not perform their risk analysis frequently, this suggest that they are not up to date with newly introduced threats. As a result, they are prone to various types of newly introduced security related risks. Therefore, it is recommended that the organisations perform a risk analysis process more frequently.

6. While findings show that organisations have a level of interest and put in some investment towards POPIA compliance, literature also requires that organisations who are compelled to have a data privacy legislation must have a formalised organisational structure which is tasked for the POPIA needs specific. Therefore, organisations must appoint a competent person who will oversee the work required by the legislation. This is who the regulation refers to as the accountable person.

7. The literature section has proven to us that information security and the POPIA are tightly aligned. In addition to this, information security weaknesses grow regularly, and require an organisation to be proactive towards defending its information security. While this is the case, it is imperative that organisations treat information security proactively and employ updated mechanisms and

procedures. This includes best practices and frameworks in place, as new efficient methods are introduced, new mechanisms are required within organisations when aligning to the POPIA needs.

8. An organisation that does not have the complete resources to fulfil the requirements of the POPIA independently, may find a third-party organisation with expertise in the field to carry the POPIA task for them. These organisations can be appointed but must have a sold legally binding contract which compels them to manage the organisations POPIA need.

9. The POPIA document alone is not sufficient. An organisation needs to investigate other existing data privacy regulations, such as the GDPR, and follow best practices adopted for GDPR compliance.

10. The cost of non-compliance with data privacy legislation may affect your organisation's operations or have certain members of your organisation arrested. Therefore, as an organisation you need to take the POPIA legislation seriously and implement the requirements correctly. This is because the legislation informs us that imprisonment is one of the repercussions, and findings have indicated that most SMEs are not aware of this. In addition, literature has proven that it is heavily expensive to avoid the imprisonment sanction which in the legislation.

12. It was found that employees or consultants who assist SMEs with developing the e-commerce site perform more than a single role in the organisation. In such instances, it is prudent to bring in POPIA experts to assist with implementation, as they are better informed and specialised.

REFERENCES

Abel, M. (2020) *OPINIONISTA: An open letter to President Ramaphosa: It's time to deliver*, *Daily Maverick*. Available at: https://www.dailymaverick.co.za/opinionista/2020-01-31-an-open-letter-topresident-ramaphosa-its-time-to-deliver/ (Accessed: 1 May 2020).

Abraham, R. (1999) *E-commerce and security: the options*, *ITWeb*. ITWeb. Available at: https://www.itweb.co.za/content/GxwQDq1A4lbqlPVo (Accessed: 30 April 2020).

Accenture (2019) *How South Africa's retailers can pivot to digital consumers*, *Accenture*. Available at: https://www.accenture.com/za-en/insights/retail/ecommerce (Accessed: 30 April 2020).

Alkalay, A. (2020) *Information Regulator Nudges President to Proclaim The Remainder of the POPIA*, *Endcode April 2020*. Endcode April 2020. Available at: https://www.endcode.org/post/informationregulator-nudges-president-to-proclaim-the-remainder-of-the-popia (Accessed: 1 May 2020).

Amazon (2018) *Amazon*, *Amazon*. Available at: https://g.co/kgs/Svd2aM (Accessed: 1 May 2020).

Amin, S., Kansana, K. and Majid, J. (2016) 'A Review Paper on E-Commerce', in *TIMS 2016International Conference*. unknown. Available at: http://dx.doi.org/ (Accessed: 30 April 2020).

Andress, J. (2014) *The Basics of Information Security | ScienceDirect*.

Anita (2017) *What is ISMS and how will it impact your business? - Anitech Consulting*, *Anitech Consulting*. Available at: https://www.anitechconsulting.com.au/what-is-isms-and-how-will-it-impactyour-business/ (Accessed: 1 May 2020).

Arewa, W. (2019) *Massive penalties for data breaches, IOL | News that Connects South Africans*. Available at: https://www.iol.co.za/business-report/companies/massive-penalties-for-data-breaches31822314 (Accessed: 1 May 2020).

Authors, G. (2019) *The Basic Security Measures Every E-Commerce Website Owner Needs | ECCouncil Official Blog*, *EC-Council Official Blog*. Available at: https://blog.eccouncil.org/the-basicsecurity-measures-every-e-commerce-website-owner-needs/ (Accessed: 1 May 2020).

Berry, A. *et al.* (2002) 'The economics of SMMEs in South Africa'. unknown. Available at: http://dx.doi.org/ (Accessed: 30 April 2020).

Botha, J. G. *et al.* (2015) 'The Effects of the PoPI Act on Small and Medium Enterprises in South Africa', in *ISSA 2015*. unknown. doi: 10.1109/ISSA.2015.7335054.

Botha, J. and Grobler, M. (2017) 'A High-Level Comparison between the South African Protection of Personal Information Act and International Data Protection Laws', in *The 12th International Conference on Cyber Warfare and Security (ICCWS)*. unknown. Available at: http://dx.doi.org/ (Accessed: 1 May 2020).

Bridgwater, A. (2018) *The 13 Types Of Data*, *Forbes*. Forbes. Available at: https://www.forbes.com/sites/adrianbridgwater/2018/07/05/the-13-types-of-data/ (Accessed: 30 April 2020).

Burns, Y. and Burger-Smidt, A. (no date) *A Commentary on the Protection of Personal Information Act*. Available at: https://store.lexisnexis.co.za/products/a-commentary-on-the-protection-of-personalinformation-act-skuZASKUPG3361 (Accessed: 1 May 2020).
Cisco (2016) *What Is IT Security? - Information Technology Security*, *Cisco*. Cisco. Available at: https://www.cisco.com/c/en/us/products/security/what-is-it-security.html (Accessed: 30 April 2020).

Chiang, I.-C. A., Jhangiani, R. S. and Price, P. C. (2015) 'Research Methods in Psychology'. BCcampus. Available at: https://opentextbc.ca/researchmethods/chapter/reliability-and-validity-ofmeasurement/ (Accessed: 10 August 2020).

Crouth, G. (2020) *Popi Act delay may leave your data vulnerable, IOL | News that Connects South Africans*. Available at: https://www.iol.co.za/personal-finance/popi-act-delay-may-leave-your-datavulnerable-43426603 (Accessed: 1 May 2020).

Creswell(2017).Available at: https://ro.ecu.edu.au/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1097&context=ism (Accessed: 1 May 2020).

cyberinsiders (2019) *A Brief History of Cybersecurity - Cybersecurity Insiders*, *Cybersecurity Insiders*. Available at: https://www.cybersecurity-insiders.com/a-brief-history-of-cybersecurity/ (Accessed: 30 April 2020).

Dala, P. (2017) *A framework and model of operation for electronic personal information to achieve and maintain compliance with Condition 7 of the Protection of Personal Information (POPI) Act*. University of Pretoria. Available at: http://hdl.handle.net/2263/61578 (Accessed: 9 December 2019).

Davidovic, D. (2014) *Silver Linings: 10 Business Benefits of Your Compliance Program*. Available at: https://www.pm360online.com/silver-linings-10-business-benefits-of-your-compliance-program/ (Accessed: 1 May 2020).

Donnelly, L. *et al.* (2018) *Another day, another data breach - The Mail & Guardian, The Mail & Guardian*. Available at: https://mg.co.za/article/2018-06-22-another-day-another-data-breach/ (Accessed: 1 May 2020).

Dutton, J. (2019) *What is an ISMS? 9 reasons why you should implement one - IT Governance UK Blog, IT Governance UK Blog*. Available at: https://www.itgovernance.co.uk/blog/what-is-an-ismsand-9-reasons-why-you-should-implement-one (Accessed: 1 May 2020).

Duane Nicol. (2019) Cybersecurity during the Covid pandemic

Elin, J. (2020) *Govt looks to cloud to accelerate service delivery, ITWeb*. Available at: https://www.itweb.co.za/content/kYbe97XDkdo7AWpG (Accessed: 14 October 2021).

Encrypt, S. (2017) *What is Encryption & How Does It Work?, Medium*. Search Encrypt. Available at: https://medium.com/searchencrypt/what-is-encryption-how-does-it-work-e8f20e340537 (Accessed: 1 May 2020).

Fatoki, O. *et al.* (2011) *Definition of small and medium enterprises in South Africa, ResearchGate*. Available at: https://www.researchgate.net/figure/Definition-of-small-and-medium-enterprises-inSouth-Africa_tbl1_266871172 (Accessed: 30 April 2020).

Forde, S. H. S. (2015) 'Trust and distrust on the web: User experiences and website characteristics', *Computers in human behavior*. Pergamon, 45, pp. 39–50.

Fruhlinger, J. (2020) *What is information security? Definition, principles, and jobs, CSO Online*. Available at: https://www.csoonline.com/article/3513899/what-is-information-security-definitionprinciples-and-jobs.html (Accessed: 30 April 2020).
Fynn, M. (2018) *Data breaches: What is required? - POPI and GDPR, Insights into The Law in South Africa | Welcome to Go Legal*. Available at: https://www.golegal.co.za/data-breaches-privacy-laws/ (Accessed: 1 May 2020).

Gernetzky, K. (2019) *Liberty Holdings reports healthy new business flows, BusinessLIVE*. Business Day. Available at: https://www.businesslive.co.za/bd/companies/financial-services/2019-11-22liberty-holdings-reports-healthy-new-business-flows/ (Accessed: 3 May 2020).

Goosen, R. and Rudman, R. (2013) 'An Integrated Framework to Implement It Governance Principles at A Strategic And Operational Level For Medium-To Large-Sized South African Businesses'. unknown, 12(7), p. 835.

Gous, N. (2017) *Top real estate company admits to being unwitting source of country's largest personal data breach, TimesLIVE*. TimesLIVE. Available at: https://www.timeslive.co.za/news/southafrica/2017-10-18-top-real-estate-company-admits-to-being-unwitting-source-of-countrys-largestpersonal-data-breach/ (Accessed: 9 December 2019).

Grid (2018) *How to get HTTPS: Setting up SSL on your website, 1-grid*. Available at: https://support.1grid.com/support/solutions/articles/33000242183-how-to-get-https-setting-up-ssl-on-your-website (Accessed: 1 May 2020).

Guide, E. (2020) *What is Ecommerce in 2020? Ecommerce Definition Explained with Examples*, *Ecommerce Guide*. Available at: https://ecommerceguide.com/guides/what-is-ecommerce/ (Accessed: 30 April 2020).

Guides, S. (2019) *PCI DSS Compliance Requirements Guide & Checklist | Sucuri*, *Sucuri*. Available at: https://sucuri.net/guides/pci-compliance-requirements-checklist/ (Accessed: 1 May 2020).

Ian Jacobsberg, L. A. (2019) *South Africa Data Protection Regulations Expected to Take Effect in 2019 | HL Chronicle of Data Protection*, *HL Chronicle of Data Protection*. Available at: https://www.hldataprotection.com/2019/04/articles/international-eu-privacy/south-africa-dataprotection-regulations-expected-to-take-effect-in-2019/ (Accessed: 3 May 2020).

ICA (2018) *What is Compliance? | ICA*, *International Compliance Association*. Available at: https://www.int-comp.org/careers/your-career-in-compliance/what-is-compliance/ (Accessed: 1 May 2020).

InfoReg (2013) *Documents*. Available at: https://www.justice.gov.za/inforeg/docs/InfoRegSA-act2013-004.pdf (Accessed: 1 May 2020).

Information Regulator (2013a) *Home l InfoRegSA*. Available at: https://www.justice.gov.za/inforeg/ (Accessed: 9 December 2019).

Information Regulator (2013b) *Information Regulator South Africa | Privacy law | POPIA*. Available at: http://www.popiact-compliance.co.za/popia-information/12-information-regulator (Accessed: 9 December 2019).

IS News (2020) *will this be the year we see the popi act come into effect?*, *Mobius Consulting*. Available at: https://mobiusconsulting.co.za/will-this-be-the-year-we-see-the-popi-act-come-into-effect/ (Accessed: 3 May 2020).

ITWeb and Weidemann, R. (2018) *Data analytics provides an answer to POPI challenges*, *ITWeb*. ITWeb. Available at: https://www.itweb.co.za/content/rxP3jMBplW5vA2ye (Accessed: 1 May 2020).
Jefferson, M. and Stephens, S. (2019) *South African data protection law and third-party processors | | Insights | DLA Piper Global Law Firm*, *DLA Piper*. Available at: https://www.dlapiper.com/en/saudiarabia/insights/publications/2019/04/africa-connected-issue2/south-african-data-protection-law-and-third-party-processors/ (Accessed: 1 May 2020).

Jougleux, P. (2012) 'Identity theft and internet', *International Journal of Liability and Scientific Enquiry*. Inderscience, 5(1), pp. 37–45.

Jumia Group | Jumia Expand Your Horizons (no date) *Jumia Group | Jumia Expand Your Horizons*. Available at: https://group.jumia.com/ (Accessed: 1 May 2020).

Kaapu, T. and Paakki, M.-K. (2006) 'Trust, Risk, Privacy, and Security in eCommerce', *FRONTIERS OF E-BUSINESS RESEARCH*, p. 3.

Kagan, J. (2015) *PCI Compliance*, *Investopedia*. Investopedia. Available at: https://www.investopedia.com/terms/p/pci-compliance.asp (Accessed: 2 May 2020).

Kandeh, A. T. (2018) 'Enforcement of the Protection of Personal Information (POPI) Act: Perspective of data management professionals', *South African Journal of Information Management*. Available at: http://www.scielo.org.za/pdf/sajim/v20n1/18.pdf (Accessed: 1 May 2020).

Kaspersky (2020) *Phishing Prevention Tips, www.kaspersky.com*. Available at: https://www.kaspersky.com//resource-center/definitions/what-is-cyber-security (Accessed: 30 April 2020).

Kothari, K. (2019) *How does SSL/TLS make HTTPS secure?, Medium*. HackerNoon.com. Available at: https://medium.com/hackernoon/how-does-ssl-tls-make-https-secure-d247bd4e4cae (Accessed: 1 May 2020).

Kraft, T. A. and Kakar, R. (2009) 'E-Commerce Security', in *CONISAR 2009*. unknown. Available at: http://dx.doi.org/ (Accessed: 30 April 2020).

Kulakov, Y. (2019) *Cyber Security in e Commerce | E-Commerce News and Guides*. Available at: https://www.cs-cart.com/blog/top-ecommerce-cyber-threats-to-be-aware-of-in-2019/ (Accessed: 2 May 2020).

Kumar, M. (2019) *Hackers infect e-commerce sites by compromising their advertising partner, The Hacker News*. Available at: https://thehackernews.com/2019/01/magecart-hacking-credit-cards.html (Accessed: 2 May 2020).

Lacey, D. and PaulSalmon (2015) 'Taking the Bait: A Systems Analysis of Phishing Attacks', *Procedia Manufacturing*. Elsevier, 3, pp. 1109–1116.

Magubane, K. (2018) *Data breach under control and under investigation, says Liberty CEO, Fin24*. Available at: https://www.fin24.com/Companies/Financial-Services/data-breach-under-control-andunder-investigation-says-liberty-ceo-20180617 (Accessed: 3 May 2020).

Michalsons (2019) *Information Regulator in South Africa, Michalsons*. Available at: https://www.michalsons.com/blog/information-regulator-in-south-africa/13893 (Accessed: 1 May 2020).

Michalsons (2020) *Transfers of Personal Information outside South Africa - Michalsons, Michalsons*. Available at: https://www.michalsons.com/focus-areas/privacy-and-data-protection/transfers-ofpersonal-information-outside-south-africa (Accessed: 1 May 2020).
mimecast (no date) *The Impact of COVID-19 on Cyber Security Insurance*. Available at: https://www.mimecast.com/nl/blog/the-impact-of-covid-19-on-cyber-security-insurance/ (Accessed: 14 October 2021).

Moyo, A. (2019) *SA's average data breach cost jumps to R43.3m, ITWeb*. ITWeb. Available at: https://www.itweb.co.za/content/KPNG8v8d3W8v4mwD (Accessed: 1 May 2020).

Moyo, A. (2020) *Regulator wants POPIA in force by Q2 2020, ITWeb*. ITWeb. Available at: https://www.itweb.co.za/content/KPNG8v8dandv4mwD (Accessed: 1 May 2020).

MPREM (2017) *Practical Challenges of Complying with POPI - M. Prem Inc - Specialists in Business Law > Publications*. Available at: http://mprem.co.za/Publications/post/practical-challenges-ofcomplying-with-popi (Accessed: 1 May 2020).

Mzekandaba, S. (2019) *Top-level UN human rights role gives Tlakula extra digital power, ITWeb*. ITWeb. Available at: https://www.itweb.co.za/content/wbrpOMgPlrgqDLZn (Accessed: 1 May 2020).

Ngalonkulu, M. (2019) E-commerce sales in SA grow 20-35% annually, Moneyweb. Available at: https://www.moneyweb.co.za/news/south-africa/e-commerce-sales-in-sa-grow-20-35-annually/ (Accessed: 30 April 2020).

Niselow, T. (2018) *Five massive data breaches affecting South Africans*, *Fin24*. Available at: https://m.fin24.com/Companies/ICT/five-massive-data-breaches-affecting-south-africans-20180619-2 (Accessed: 1 May 2020).

OECD (2011). Available at: https://ro.ecu.edu.au/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1097&context=ism (Accessed: 1 May 2020).

PayGate (2017) *Ensuring Security for Your Online Transactions*, *PayGate*. Available at: https://www.paygate.co.za/ensuring-security-online-transactions/ (Accessed: 1 May 2020).

PaySpace (2021) *How POPIA will impact cloud providers.* Available at: https://www.payspace.com/how-popia-will-impact-cloud-providers/ (Accessed: 19 October 2021).

PayU (2017) *A Guide to South Africa's eCommerce Laws*, *Source: https://www.payu.co.za/blog/guidesouth-africas-ecommerce-laws © PayU*. Available at: https://www.payu.co.za/blog/guide-southafricas-ecommerce-laws (Accessed: 1 May 2020).

Peters, J. (no date) *Celebrate Data Privacy Day by Sharing These Free Resources!* Available at: https://resources.infosecinstitute.com/topic/celebrate-data-privacy-day-by-sharing-these-freeresources/ (Accessed: 14 October 2021).

Pillay, P. by C. (2014) *What SMEs need to know about the POPI Act | SME South Africa*, *SME South Africa*. Available at: https://smesouthafrica.co.za/What-SMEs-need-to-know-about-the-POPI-Act/ (Accessed: 1 May 2020).

Piper, D. L. A. (2020) *DLA Piper Global Data Protection Laws of the World - World Map, DATA PROTECTION LAWS OF THE WORLD*. Available at: https://www.dlapiperdataprotection.com/ (Accessed: 1 May 2020).

Privacy by Design - The 7 Foundational Principles (no date). Available at: https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/ (Accessed: 14 October 2021).

PixelPin (2018) *Cybersecurity is becoming more and more expensive*, *Medium*. Medium. Available at: https://medium.com/@PixelPin/cybersecurity-is-becoming-more-and-more-important-381dcbab7859 (Accessed: 2 May 2020).

POPIA (Pty) Ltd (2015) *POPIA Compliance Framework and Monitoring System, IT Gov*. Available at: https://www.itgovernance.co.za/3/index.php/popi-act/125-popia/202-popi-act-compliance-framework (Accessed: 1 May 2020).

Randhawa, M. (2019) *How can you Measure Organisational Culture?* myHRfuture. Available at: https://www.myhrfuture.com/blog/2019/7/19/how-can-you-measure-organisational-culture (Accessed: 19 October 2021).

Regan, J. (2017) *What is Malware? How Malware Works & How to Remove It*. Available at: https://www.avg.com/en/signal/what-is-malware (Accessed: 3 May 2020).

Reuters (2018) *Amazon 'considers' setting up insurance comparison site in UK*, *the Guardian*. Available at: http://www.theguardian.com/business/2018/aug/16/amazon-considers-setting-upinsurance-comparison-site-in-uk (Accessed: 1 May 2020).

Rieck, K. A., Korolev, I. A. and Barker, A. V. (2008) 'Centralized Payment Gateway System and Method', *US Patent*. Available at:

https://patentimages.storage.googleapis.com/0b/c5/8d/ee65b82095d492/US20080103923A1.pdf (Accessed: 1 May 2020).

Right2Know (2016) *Right2Know*. Available at: https://privacyinternational.org/sites/default/files/2018-04/South%20Africa_UPR_Stakeholder%20Report_Right%20to%20Privacy.pdf (Accessed: 1 May 2020).

Right2Know (2018) *State of Privacy South Africa*, *Privacy International*. Available at: https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa (Accessed: 1 May 2020).

Rocket, M. (2018) *PoPI vs. GDPR*, *Medium*. Black Ink Advisory. Available at: https://medium.com/black-ink-advisory/popi-vs-gdpr-956093118061 (Accessed: 1 May 2020).

Rouse, M. (2020) *What is Ransomware and How Do You Remove It?*, *SearchSecurity*. TechTarget. Available at: https://searchsecurity.techtarget.com/definition/ransomware (Accessed: 3 May 2020).

Rubin, S. H. (2011) 'Distributed denial-of-service attacks - IEEE Conference Publication', *IEEE Xplore Digital Library*. Available at: https://ieeexplore.ieee.org/document/886455 (Accessed: 1 May 2020).

Saal, P. (2018) 'Data leak exposes personal records of nearly 1 million South Africans'. Available at: https://www.timeslive.co.za/news/sci-tech/2018-05-24-data-leak-exposes-personal-records-of-nearly1-million-south-africans/ (Accessed: 1 May 2020).

Sadler, J. M. (2015) *8 Tips to Reduce the Risk of a Cyber Attack - SADLER & Company, Inc*, *SADLER & Company, Inc*. SADLER and Company, Inc. Available at: https://www.sadlerco.com/8-tips-toreduce-the-risk-of-a-cyber-attack/ (Accessed: 1 May 2020).

Shapshak, T. (2018) *Liberty hack the 'biggest breach yet'*, *BusinessLIVE*. Financial Mail. Available at: https://www.businesslive.co.za/fm/fm-fox/2018-06-21-liberty-hack-the-biggest-breach-yet/ (Accessed: 3 May 2020).

Shedden, P. (2010) 'Information Security Risk Assessment: Towards a Business Practice Perspectiv', in. Edith Cowan University . Available at: https://ro.ecu.edu.au/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1097&context=ism (Accessed: 1 May 2020).

Signé, L. and Signé, K. (2018) *Cybersecurity in Africa: Securing businesses with a local approach with global standards*, *Brookings*. Brookings. Available at: https://www.brookings.edu/blog/africa-infocus/2018/06/04/cybersecurity-in-africa-securing-businesses-with-a-local-applicationroach-withglobal-standards/ (Accessed: 3 March 2020).

Sikhungo, M. (2015) *POPI series - condition 7 - information security - Dommisse Attorneys Inc*, *Dommisse Attorneys Inc.* Available at: https://dommisseattorneys.co.za/blog/popi-series-condition-7information-security/ (Accessed: 1 May 2020).

Skrba, A. (2019) *The Beginner's Guide to Content Delivery Networks - 2020*. Available at: https://firstsiteguide.com/cdn-guide/ (Accessed: 2 May 2020).

Simons (2020) defining consent in commercial online application.

Zadig (2010) 'Securing IS assets through hacker deterrence: A case study - IEEE Conference Publication', in *eCrime Researchers Summit*, pp. 1–7.

Strachan, F. (2008) ‘Mobile Operating System - an overview | ScienceDirect Topics’, *Science Direct*. Available at: https://www.sciencedirect.com/topics/computer-science/mobile-operating-system (Accessed: 3 May 2020).

Suchacka, G. (2020) ‘Identifying legitimate Web users and bots with different traffic profiles — an Information Bottleneck approach’, *Knowledge-Based Systems*. Elsevier, 197, p. 105875.

Supplied (2018) *Why SMEs need different rules to big businesses, IOL | News that Connects South Africans*. Available at: https://www.iol.co.za/business-report/economy/why-smes-need-different-rulesto-big-businesses-18366772 (Accessed: 2 May 2020).

Sobers, R. (2020) *98 Must-Know Data Breach Statistics for 2021*. Available at: https://www.varonis.com/blog/data-breach-statistics/ (Accessed: 15 October 2021).

Takealot.com (2019) *About - Takealot.com*. Available at: https://www.takealot.com/about/our-journey/ (Accessed: 1 May 2020).

Tomlinson, M. (2009) ‘Tackling E-commerce Security Issues Head On’, *Computer Fraud & Security*. Elsevier Advanced Technology, 2000(11), pp. 10–13.

Tumber, R. (2019) *3 Compelling Reasons To Invest In Cyber Security - Part 1, Forbes*. Forbes. Available at: https://www.forbes.com/sites/rajindertumber/2019/01/12/3-compelling-reasons-toinvest-in-cyber-security-part-1/ (Accessed: 30 April 2020).

Varghese, J. (2020) *IT Security Audit: Types, Importance and Methodology, Astra Security Blog*. Available at: https://www.getastra.com/blog/security-audit/it-security-audit/ (Accessed: 1 May 2020).

Wang, S. S. (2019) ‘Integrated framework for information security investment and cyber insurance’, *Pacific-Basin Finance Journal*. North-Holland, 57, p. 101173.

Xperien (2020) *It’s time to act on POPIA*. Available at: https://www.fanews.co.za/article/complianceregulatory/2/general/1082/it-s-time-to-act-on-popia/28351 (Accessed: 1 May 2020).

Ablon, L., Heaton, P., Lavery, D., & Romanosky, S. (2016). *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*. https://doi.org/10.7249/rr1187

DeFranzo, S. E. (2011, September 16). Difference between qualitative and quantitative research. Retrieved December 12, 2019, from Snap Surveys Blog website: https://www.snapsurveys.com/blog/qualitative-vs-quantitative-research/

De Stadler, E., & Esselaar, P. (2015). *A Guide to the Protection of Personal Information Act*.

Gratton, E. (n.d.). If Personal Information is Privacy’s Gatekeeper, then Risk of Harm is the Key: A Proposed Method for Determining What Counts as Personal Information. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2334938

Information Regulator. (2013a). Home l InfoRegSA. Retrieved December 9, 2019, from https://www.justice.gov.za/inforeg/

Information Regulator. (2013b). Information Regulator South Africa | Privacy law | POPIA. Retrieved December 9, 2019, from http://www.popiact-compliance.co.za/popia-information/12-informationregulator

ISACA. (2012). *COBIT 5 for Information Security*. ISACA.

Isaca. (2014). *Securing Mobile Devices Using COBIT 5 for Information Security*.

Kersten, H., Reuter, J., & Schröder, K.-W. (2013). Das ISMS nach ISO 27001. *IT-Sicherheitsmanagement Nach ISO 27001 Und Grundschutz*, pp. 45–108. https://doi.org/10.1007/9783-658-01724-8_3

Michalsons. (n.d.). Protection of Personal Information Act Summary | POPIA. Retrieved December 9, 2019, from Michalsons website: https://www.michalsons.com/focus-areas/privacy-and-dataprotection/protection-of-personal-information-act-popia

PwC (2011) *popi white paper*. Available at: https://www.pwc.co.za/en/assets/pdf/popi-white-paper2011.pdf (Accessed: 1 May 2020).

Rogerson, C. (2018). *Local Economic Development in the Changing World: The Experience of Southern Africa*. Routledge.

Singh, S. (2003). Stratified and Post-Stratified Sampling. *Advanced Sampling Theory with Applications*, pp. 649–764. https://doi.org/10.1007/978-94-007-0789-4_8

Staunton, C., Adams, R., Botes, M., Dove, E. S., Horn, L., Labuschaigne, M., … De Vries, J. (2019). Safeguarding the future of genomic research in South Africa: Broad consent and the Protection of Personal Information Act No. 4 of 2013. *South African Medical Journal = Suid-Afrikaanse Tydskrif Vir Geneeskunde*, *109*(7), 468–470.

Taylor, D., & Cronjé, F. (2014). *101 Questions and Answers about: The Protection of Personal Information Act*. Juta and Company Ltd.

The Law The Law Library. (2018). *Act on the Protection of Personal Information (Japan) (2018 Edition)*. Createspace Independent Publishing Platform.

Chiang, I.-C. A., Jhangiani, R. S. and Price, P. C. (2015) 'Research Methods in Psychology'. BCcampus. Available at: https://opentextbc.ca/researchmethods/chapter/reliability-and-validity-ofmeasurement/ (Accessed: 10 August 2020).
Data Privacy Manager (2020). Available at: https://dataprivacymanager.net/ (Accessed: 14 October 2021).

Damaskinidis, G. (2017) 'Qualitative Research and Subjective Impressions in Educational Contexts', *Journal of educational and behavioral statistics: a quarterly publication sponsored by the American Educational Research Association and the American Statistical Association*. Science and Education Publishing, 5(12), pp. 1228–1233.

Doyle, A. (2020) *What Is a Semi-Structured Interview?* Available at: https://www.thebalancecareers.com/what-is-a-semi-structured-interview-2061632 (Accessed: 10 August 2020).

Giacobbi, P. R., Jr. (2011) *A Pragmatic Research Philosophy for Applied Sport Psychology*. Available at: https://digitalcommons.brockport.edu/cgi/viewcontent.cgi?article=1079&context=pes_facpub (Accessed: 10 August 2020).

Gill, P. *et al.* (2008) 'Methods of data collection in qualitative research: interviews and focus groups', *British dental journal*. Nature Publishing Group, 204(6), pp. 291–295.

Hashmi, F. K. *et al.* (2017) 'A qualitative study exploring perceptions and attitudes of community pharmacists about extended pharmacy services in Lahore, Pakistan', *BMC health services research*. BioMed Central, 17(1), pp. 1–9.

Horton, M. (2020) *Simple Random Sample: Advantages and Disadvantages*. Available at: https://www.investopedia.com/ask/answers/042815/what-are-disadvantages-using-simple-randomsample-approximate-larger-population.asp (Accessed: 10 August 2020).

Institute of Lifelong Learning (2009) *9. The advantages and disadvantages of questionnaires*. Available at: https://www.le.ac.uk/oerresources/lill/fdmvco/module9/page_51.htm (Accessed: 10 August 2020).

Isaca (2014) *Securing Mobile Devices Using COBIT 5 for Information Security*.

Jamie Hale, M. S. (2011) *The 3 Basic Types of Descriptive Research Methods*. Available at: https://psychcentral.com/blog/the-3-basic-types-of-descriptive-research-methods/ (Accessed: 10 August 2020).

(John Dudovskiy, nd). (no date) *Exploratory Research*. Available at: https://researchmethodology.net/research-methodology/research-design/exploratory-research/ (Accessed: 10 August 2020).

Jorge Faber, L. M. F. (2014) 'How sample size influences research outcomes', *Dental press journal of orthodontics*. Dental Press International, 19(4), p. 27.

Judith Schoonenboom, R. B. J. (2017) 'How to Construct a Mixed Methods Research Design', *Kolner Zeitschrift fur Soziologie und Sozialpsychologie*. Springer, 69(Suppl 2), p. 107.

Krieger, N. (2012) 'Who and What Is a "Population"? Historical Debates, Current Controversies, and Implications for Understanding "Population Health" and Rectifying Health Inequities', *The Milbank quarterly*. Milbank Memorial Fund, 90(4), p. 634.

Lavrakas, P. J. (2008) *Face-to-Face Interviewing, Face-to-Face Interviewing*. Available at: https://methods.sagepub.com/reference/encyclopedia-of-survey-research-methods/n174.xml (Accessed: 10 August 2020).

Mackinnon, A. and Powell, B. (2008) 'Paradigms and Worldviews', in *China Calling*. Palgrave Macmillan, London, pp. 23–25.

Martin (2013) Consent management in data security (Accessed: 10 August 2020).

McCombes, S. (2019) *Research Design*. Available at: https://www.scribbr.com/researchprocess/research-design/ (Accessed: 10 August 2020).

McGrath, C. (2018) *Twelve tips for conducting qualitative research interviews, https://www.tandfonline.com/doi/full/10.1080/0142159X.2018.1497149*. Available at: https://www.tandfonline.com/doi/full/10.1080/0142159X.2018.1497149 (Accessed: 10 August 2020).

Mcleod, S. (no date) *Qualitative vs Quantitative Research*. Available at: https://www.simplypsychology.org/qualitative-quantitative.html (Accessed: 10 August 2020).

Picincu, A. (2018) *The Advantages of Using a Questionnaire, bizfluent*. Available at: https://bizfluent.com/info-8206848-advantages-using-questionnaire.html (Accessed: 10 August 2020).

rvarughese (2016) *3 Types of Marketing Research Designs (Exploratory, Descriptive, Causal)*. Available at: https://wmbamarketing.wordpress.com/2016/04/08/3-types-of-marketing-researchdesigns-exploratory-descriptive-causal/ (Accessed: 10 August 2020).

Signé, L. and Signé, K. (2018) *Cybersecurity in Africa: Securing businesses with a local approach with global standards*, *Brookings*. Brookings. Available at: https://www.brookings.edu/blog/africa-infocus/2018/06/04/cybersecurity-in-africa-securing-businesses-with-a-local-approach-with-globalstandards/ (Accessed: 3 March 2020).

Steup, M. and Neta, R. (2005) 'Epistemology'. Available at: https://plato.stanford.edu/entries/epistemology/ (Accessed: 10 August 2020).

Streefkerk, R. (2019) *Qualitative vs. Quantitative Research*. Available at: https://www.scribbr.com/methodology/qualitative-quantitative-research/ (Accessed: 10 August 2020).

South Africa - Data Protection Overview (2021). Available at: https://www.dataguidance.com/notes/southafrica-dataprotection-overview (Accessed: 14 October 2021).

Thorne, S. (2000) 'Data analysis in qualitative research', *Evidence-based nursing*. Royal College of Nursing, 3(3), pp. 68–70.

van der Merwe, P. (2018) *Hawks expect 'Master Deeds' update*, *Jacaranda FM*. Available at: https://www.jacarandafm.com/news/news/hawks-expect-master-deeds-update/ (Accessed: 3 May 2020).

William, M. (2016) *Sampling*. Conjoint.ly.

Willis (2017) *[No title], World Views, Paradigms, and the Practice of Social Science Research*. Available at: https://www.sagepub.com/sites/default/files/upm-binaries/13885_Chapter1.pdf (Accessed: 10 August 2020).

Žukauskas, P., Vveinhardt, J. and Andriukaitienė, R. (2018) 'Management Culture and Corporate Social Responsibility', in *Management Culture and Corporate Social Responsibility*. IntechOpen.

ANNEXURES

Annexure 1

Consent form

Greetings:

My name is Itumeleng Moraka. I am a Masters degree candidate studying at the University of KwaZuluNatal, Westville Campus. The title of my research is: A framework for the Protection of Personal Information Act compliance in the e-commerce IT sector. My contact No is: 082 642 9787 and email address: 219095366@stu.ukzn.ac.za

You are being invited to consider participating in a study that involves filling in a survey, to share your experiences or knowledge on the subject matter. The aim and purpose of this research is to develop a frame of reference for SMEs to implement the POPIA. The study is expected to enrol 100 participants who work in the development of SME's e-commerce systems, and are based in Gauteng province, South Africa. The duration of your participation if you choose to enrol and remain in the study is expected to be 13 months.

Please note that:

* The information that you provide will be used for scholarly research only.
* There is no compensation for participating in this study.
* The study does not include any medical risks.
* Your participation is entirely voluntary. You have a choice to participate, not to participate or stop participating in the research. You will not be penalised for taking such an action.
* Your input in this will be presented anonymously. Neither your name nor identity will be disclosed in any form in the study.
* The questionnaire will take about 30 minutes.
* The record as well as other items associated with the questionnaire will be held in a passwordprotected file accessible only to myself and my supervisors. After a period of the study, in line with the rules of the university, it will be disposed of by shredding, burning or permanent deletion.

* If you agree to participate please sign the declaration attached to this statement.

This study has been ethically reviewed and approved by the UKZN Humanities and Social Sciences Research Ethics Committee (approval number).

In the event of any problems or concerns/questions you may contact the researcher at (provide contact details) or the UKZN Humanities & Social Sciences Research Ethics Committee, contact details as follows:

Before you agree or disagree to participate in the survey, please read the items below.

I been informed about the study entitled A framework for the Protection of Personal Information Act compliance in the e-commerce IT sector by Itumeleng Moraka.

I understand the purpose and procedures of the study.

I have been given an opportunity to answer questions about the study and have had answers to my satisfaction.

I declare that my participation in this study is entirely voluntary and that I may withdraw at any time without affecting any of the benefits that I usually am entitled to.

I have been informed about any available compensation or medical treatment if injury occurs to me as a result of study-related procedures.

If I have any further questions/concerns or queries related to the study I understand that I may contact the researcher is: 082 642 9787 and email address: 219095366@stu.ukzn.ac.za

If I have any questions or concerns about my rights as a study participant, or if I am concerned about an aspect of the study or the researchers then I may contact:

HUMANITIES & SOCIAL SCIENCES RESEARCH ETHICS ADMINISTRATION
Research Office, Westville Campus
Govan Mbeki Building
Private Bag X 54001
Durban
4000
KwaZulu-Natal, SOUTH AFRICA
Tel: 27 31 2604557 - Fax: 27 31 2604609
Email: HSSREC@ukzn.ac.za

Annexure 2

Output tables

Section A Demographics

1. Your gender?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	56	65.1	65.1	65.1
	Female	30	34.9	34.9	100.0
	Total	86	100.0	100.0	

2. Your age?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	20-25	4	4.7	4.7	4.7
	26-30	15	17.4	17.4	22.1
	31-35	33	38.4	38.4	60.5
	35-40	26	30.2	30.2	90.7
	41-45	8	9.3	9.3	100.0
	Total	86	100.0	100.0	

3.1 Information security implementation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	50	58.1	58.1	58.1
	No	36	41.9	41.9	100.0
	Total	86	100.0	100.0	

3.2 Software developer

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	59	68.6	68.6	68.6
	No	27	31.4	31.4	100.0
	Total	86	100.0	100.0	

3.3 Project manager

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	46	53.5	53.5	53.5
	No	40	46.5	46.5	100.0
	Total	86	100.0	100.0	

3.4 Database administrator / designer

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	40	46.5	46.5	46.5
	No	46	53.5	53.5	100.0
	Total	86	100.0	100.0	

4. How long have you worked in the field?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	<1 year	1	1.2	1.2	1.2
	1 - <3 years	10	11.6	11.6	12.8
	3-4 years	50	58.1	58.1	70.9
	>4 years	25	29.1	29.1	100.0
	Total				

	86	100.0	100.0	

5. Indicate your awareness and knowledge of the POPIA legislation?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		7	8.1	8.1	8.1
	I have heard of POPIA and know a little about it	79		91.9	100.0
	I have heard of POPIA and know a lot about it		91.9		
	Total	86	100.0	100.0	

1.1 COBIT 5

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid					
	Yes	81	94.2	94.2	94.2
	No	5	5.8	5.8	100.0
	Total	86	100.0	100.0	

1.2 IS0 27001 / 27002

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid					
	Yes	81	94.2	94.2	94.2
	No	5	5.8	5.8	100.0
	Total	86	100.0	100.0	

1.3 GAAP

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	1	1.2	1.2	1.2
	No	85	98.8	98.8	100.0
	Total	86	100.0	100.0	

1.4 NIST SP 800

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	5	5.8	5.8	5.8
	No	81	94.2	94.2	100.0
	Total	86	100.0	100.0	

Binomial Test

		Category	N	Observed Prop.	Test Prop.	Asymp. Sig. (2-tailed)
1.1 COBIT 5	Group 1	Yes	81	.94	.50	.000[a]
	Group 2	No	5	.06		
	Total		86	1.00		
1.2 IS0 27001 / 27002	Group 1	Yes	81	.94	.50	.000[a]
	Group 2	No	5	.06		
	Total		86	1.00		
1.3 GAAP	Group 1	No	85	.99	.50	.000[a]
	Group 2	Yes	1	.01		
	Total		86	1.00		
1.4 NIST SP 800	Group 1	No	81	.94	.50	.000[a]
	Group 2	Yes	5	.06		
	Total		86	1.00		

a. Based on Z Approximation.

2.1 Encryption

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	84	97.7	97.7	97.7
	No	2	2.3	2.3	100.0
	Total	86	100.0	100.0	

2.2 Web Application Firewall

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	79	91.9	91.9	91.9
	No	7	8.1	8.1	100.0
	Total	86	100.0	100.0	

2.3 Physical security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	69	80.2	80.2	80.2
	No	17	19.8	19.8	100.0
	Total	86	100.0	100.0	

2.4 Database audits

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	43	50.0	50.0	50.0
	No	43	50.0	50.0	100.0
	Total	86	100.0	100.0	

Binomial Test

		Category	N	Observed Prop.	Test Prop.	Asymp. Sig. (2-tailed)
2.1 Encryption	Group 1	Yes	84	.98	.50	.000[a]
	Group 2	No	2	.02		
	Total		86	1.00		
2.2 Web Application Firewall	Group 1	Yes	79	.92	.50	.000[a]
	Group 2	No	7	.08		
	Total		86	1.00		
2.3 Physical security	Group 1	Yes	69	.80	.50	.000[a]
	Group 2	No	17	.20		
	Total		86	1.00		
2.4 Database audits	Group 1	Yes	43	.50	.50	1.000[a]
	Group 2	No	43	.50		
	Total		86	1.00		

a. Based on Z Approximation.

3.1 The company provides me with adequate Information Security Training awareness

		Frequency	Percent	~~Valid Percent~~	~~Cumulative Percent~~
Valid		1	1.2	~~1.2~~	1.2
		3	3.5	~~3.5~~	4.7
	Strongly disagree Disagree Slightly disagree	9	10.5	~~10.5~~	15.1
	Slightly agree Agree Strongly agree	18	20.9	~~20.9~~	36.0
	~~Total~~	41	47.7	~~47.7~~	83.7

	14	16.3	16.3	100.0
	86	100.0	100.0	

3.2 Top management understands the contents of the POPIA legislation

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	2.3	2.3	2.3
	10	11.6	11.6	14.0
	30	34.9	34.9	48.8
	31	36.0	36.0	84.9
Disagree				
Slightly disagree				
Slightly agree	13	15.1	15.1	100.0
Agree				
Strongly agree				
Total	86	100.0	100.0	

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
3.1 The company provides me with adequate Information Security Training awareness	86	4.59	1.067	.115
3.2 Top management understands the contents of the POPIA legislation	86	4.50	.967	.104

One-Sample Test

	Test Value = 3.5					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
3.1 The company provides me with adequate Information Security Training awareness	9.501	85	.000	1.093	.86	1.32
3.2 Top management understands the contents of the POPIA legislation	9.589	85	.000	1.000	.79	1.21

Item	Responses as Frequency (%)						n	Mean (SD)	t	df	p-value
	Strongly disagree	Disagree	Slightly disagree	Slightly agree	Agree	Strongly agree					
The company provides me with adequate Information Security Training awareness	1 (1.2)	3 (3.5)	9 (10.5)	18 (20.9)	41 (47.7)	14 (16.3)	86	4.59 (1.067)	9.501	85	<.0005*

* indicates significance at the 95% level

4.1 Questionnaires

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	65	75.6	75.6	75.6
	No	21	24.4	24.4	100.0
	Total	86	100.0	100.0	

4.2 Interviews

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	24	27.9	27.9	27.9
	No	62	72.1	72.1	100.0
	Total	86	100.0	100.0	

		Category	N	Observed Prop.	Test Prop.	Asymp. Sig. (2-tailed)
4.1 Questionnaires	Group 1	No	21	.24	.50	.000[a]
	Group 2	Yes	65	.76		
	Total		86	1.00		
4.2 Interviews	Group 1	No	62	.72	.50	.000[a]
	Group 2	Yes	24	.28		
	Total		86	1.00		

Binomial Test

a. Based on Z Approximation.

5. Do you ALWAYS get consent from your customers to store and process their data?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	69	80.2	80.2	80.2
	No	17	19.8	19.8	100.0
	Total	86	100.0	100.0	

6.1 Privacy Policy statement on website

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	61	70.9	70.9	70.9
	No	25	29.1	29.1	100.0
	Total	86	100.0	100.0	

6.2 Terms and Conditions statement on website

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	59	68.6	68.6	68.6
	No	27	31.4	31.4	100.0
	Total	86	100.0	100.0	

7. Indicate which of the following actions your organisation takes MOST OFTEN to ensure that customers are informed when there is a data breach.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		9	10.5	10.5	10.5
	No action	36	41.9	41.9	52.3
	SMS / Text	17	19.8	19.8	72.1
	Call	24	27.9	27.9	100.0
	Put an announcement on the website Total				

	86	100.0	100.0	

Test Statistics

	7. Indicate which of the following actions your organisation takes MOST OFTEN to ensure that customers are informed when there is a data breach.
Chi-Square	18.279[a]
df	3
Asymp. Sig.	.000

a. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 21.5.

8. Which of the following risks do you encounter MOST OFTEN in your business? (Select ONE option)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		34	39.5	39.5	39.5
		31	36.0	36.0	75.6
	Database hack	21		24.4	100.0
	Denial-of-service attack		24.4		
	Theft of customer payment details Total	86	100.0	100.0	

8. Which of the following risks do you encounter MOST OFTEN in your business? (Select ONE option)

	Observed N	Expected N	Residual
Database hack	34	28.7	5.3
Denial-of-service attack	31	28.7	2.3
Theft of customer payment details	21	28.7	-7.7

Total	86		

Test Statistics

	8. Which of the following risks do you encounter MOST OFTEN in your business? (Select ONE option)
Chi-Square	3.233[a]
df	2
Asymp. Sig.	.199

a. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 28.7.

9.1 Access control levels

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	70	81.4	81.4	81.4
	No	16	18.6	18.6	100.0
	Total	86	100.0	100.0	

9.2. Verification process

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	65	75.6	75.6	75.6
	No	21	24.4	24.4	100.0
	Total	86	100.0	100.0	

Binomial Test

		Category	N	Observed Prop.	Test Prop.	Asymp. Sig. (2-tailed)
9.1 Access control levels		Yes	70	.81	.50	.000[a]
	Group 1	No	16	.19		
	Group 2					
	Total		86	1.00		
9.2. Verification process	Group 1	Yes	65	.76	.50	.000[a]
	Group 2	No	21	.24		
	Total		86	1.00		

a. Based on Z Approximation.

10. How frequently does your organisation update its risk analysis list? (Select ONE option only)

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	7	8.1	8.1	8.1
At least every 3 months	10	11.6	11.6	19.8
Every 3 -<6 months	12	14.0	14.0	33.7
Every 6 - <9 months	36	41.9	41.9	75.6
Every 9 - 12 months	19	22.1	22.1	97.7
Less often than every 12 months	2	2.3	2.3	100.0
Never				
Total	86	100.0	100.0	

10. How frequently does your organisation update its risk analysis list? (Select ONE option only)

	Observed N	Expected N	Residual
At least every 3 months	7	14.3	-7.3
Every 3 -<6 months	10	14.3	-4.3
Every 6 - <9 months	12	14.3	-2.3
Every 9 - 12 months	36	14.3	21.7
Less often than every 12 months	19	14.3	4.7
Never	2	14.3	-12.3

Total	86		

Test Statistics

	10. How frequently does your organisation update its risk analysis list? (Select ONE option only)
Chi-Square	50.326[a]
df	5
Asymp. Sig.	.000

a. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 14.3.

11.1 Management provides adequate support to implement the POPIA 7TH condition

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		3	3.5	3.5	3.5
		4	4.7	4.7	8.1
	Strongly disagree	10	11.6	11.6	19.8
	Disagree	22	25.6	25.6	45.3
	Slightly disagree	34	39.5	39.5	84.9
	Slightly agree	13	15.1	15.1	100.0
	Agree				
	Strongly agree				
	Total	86	100.0	100.0	

11.2 Management provides a budget to implement compliance measures

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	3	3.5	3.5	3.5

	Disagree	4	4.7	4.7	8.1
	Slightly disagree	9	10.5	10.5	18.6
	Slightly agree	24	27.9	27.9	46.5
	Agree	34	39.5	39.5	86.0
	Strongly agree	12	14.0	14.0	100.0
	Total	86	100.0	100.0	

11.3 Management employs an outside company to oversee certain aspects of the POPIA task

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		6	7.0	7.0	7.0
		11	12.8	12.8	19.8
	Strongly disagree	13	15.1	15.1	34.9
	Disagree	21	24.4	24.4	59.3
	Slightly disagree	26	30.2	30.2	89.5
	Slightly agree	9	10.5	10.5	100.0
	Agree				
	Strongly agree				
	Total	86	100.0	100.0	

11.4. Management audits our POPIA compliance

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	3	3.5	3.5	3.5
	Disagree	6	7.0	7.0	10.5
	Slightly disagree	11	12.8	12.8	23.3
	Slightly agree	23	26.7	26.7	50.0
	Agree	32	37.2	37.2	87.2
	Strongly agree				

	Total	11	12.8	12.8	100.0
		86	100.0	100.0	

11.5 Management ensures that third party organisations are also compliant

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	4	4.7	4.7	4.7
	Disagree	8	9.3	9.3	14.0
	Slightly disagree	16	18.6	18.6	32.6
	Slightly agree	18	20.9	20.9	53.5
	Agree	32	37.2	37.2	90.7
	Strongly agree	8	9.3	9.3	100.0
	Total	86	100.0	100.0	

11.6. Management provides us with up-to-date training so that we know what is right or wrong

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		3	3.5	3.5	3.5
		7	8.1	8.1	11.6
	Strongly disagree	10	11.6	11.6	23.3
	Disagree	24	27.9	27.9	51.2
	Slightly disagree	29	33.7	33.7	84.9
	Slightly agree	13	15.1	15.1	100.0
	Agree	86	100.0	100.0	
	Strongly agree				
	Total				

11.7 Management has developed policies to drive the POPIA in the organisation

	Frequency	Percent	Valid Percent	Cumulative Percent

Valid		3	3.5	3.5	3.5
		6	7.0	7.0	10.5
	Strongly disagree	11	12.8	12.8	23.3
	Disagree	25	29.1	29.1	52.3
	Slightly disagree	30	34.9	34.9	87.2
	Slightly agree	11	12.8	12.8	100.0
	Agree				
	Strongly agree				
	Total	86	100.0	100.0	

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
11.1 Management provides adequate support to implement the POPIA 7TH condition	86	4.38	1.219	.131
11.2 Management provides a budget to implement compliance measures	86	4.37	1.198	.129
11.3 Management employs an outside company to oversee certain aspects of the POPIA task	86	3.90	1.423	.153
11.4. Management audits our POPIA compliance	86	4.26	1.248	.135
11.5 Management ensures that third party organisations are also compliant	86	4.05	1.319	.142
11.6. Management provides us with up-to-date training so that we know what is right or wrong	86	4.26	1.285	.139
11.7 Management has developed policies to drive the POPIA in the organisation	86	4.23	1.243	.134

One-Sample Test

	Test Value = 3.5					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
11.1 Management provides adequate support to implement the POPIA 7TH condition	6.722	85	.000	.884	.62	1.15
11.2 Management provides a budget to implement compliance measures	6.748	85	.000	.872	.62	1.13
11.3 Management employs an outside company to oversee certain aspects of the POPIA task	2.577	85	.012	.395	.09	.70
11.4. Management audits our POPIA compliance	5.617	85	.000	.756	.49	1.02
11.5 Management ensures that third party organisations are also compliant	3.843	85	.000	.547	.26	.83
11.6. Management provides us with up-to-date training so that we know what is right or wrong	5.454	85	.000	.756	.48	1.03
				.733		

11.7 Management has developed policies to drive the POPIA in the organisation	5.465	85	.000		.47	1.00

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
MANSUP	86	4.2060	1.11211	.11992

One-Sample Test

	Test Value = 3.5					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
MANSUP	5.887	85	.000	.70598	.4675	.9444

12.1 Reputational Damage

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	1	1.2	1.2	1.2
	Slightly disagree	2	2.3	2.3	3.5
	Slightly agree	8	9.3	9.3	12.8
	Agree	53	61.6	61.6	74.4
	Strongly agree				

	Total	22	25.6	25.6	100.0
		86	100.0	100.0	

12.2 Imprisonment

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	1.2	1.2	1.2
		2	2.3	2.3	3.5
	Strongly disagree	5	5.8	5.8	9.3
	Disagree	11	12.8	12.8	22.1
	Slightly disagree	54	62.8	62.8	84.9
	Slightly agree	13	15.1	15.1	100.0
	Agree				
	Strongly agree				
	Total	86	100.0	100.0	

12.3 Loss of customer confidence

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Slightly disagree	3	3.5	3.5	3.5

	Slightly agree	8	9.3	9.3	12.8
	Agree	45	52.3	52.3	65.1
	Strongly agree	30	34.9	34.9	100.0
	Total	86	100.0	100.0	

12.4 Heavy fines

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		3	3.5	3.5	3.5
	Slightly disagree	10	11.6	11.6	15.1
	Slightly agree	48	55.8	55.8	70.9
	Agree	25	29.1	29.1	100.0
	Strongly agree				
	Total	86	100.0	100.0	

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
12.1 Reputational Damage	86	5.08	.739	.080
12.2 Imprisonment	86	4.79	.935	.101
12.3 Loss of customer confidence	86	5.19	.744	.080

12.4 Heavy fines	86	5.10	.736	.079

One-Sample Test

	Test Value = 3.5					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
12.1 Reputational Damage	19.843	85	.000	1.581	1.42	1.74
12.2 Imprisonment	12.808	85	.000	1.291	1.09	1.49
12.3 Loss of customer confidence	21.022	85	.000	1.686	1.53	1.85
12.4 Heavy fines	20.216	85	.000	1.605	1.45	1.76

One-Sample Test

	Test Value = 3.5					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
12.1 Reputational Damage	19.843	85	.000	1.581	1.42	1.74
12.2 Imprisonment	12.808	85	.000	1.291	1.09	1.49
12.3 Loss of customer confidence	21.022	85	.000	1.686	1.53	1.85
12.4 Heavy fines	20.216	85	.000	1.605	1.45	1.76

One-Sample Statistics

Mean	Std. Deviation	Std. Error Mean
5.1240	.70116	.07561

One-Sample Test

	Test Value = 3.5

df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
			Lower	Upper
85	.000	1.62403	1.4737	1.7744

13.1 Maintain a strong reputation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		8	9.3	9.3	9.3
	Slightly disagree	1	1.2	1.2	10.5
	Slightly agree	55	64.0	64.0	74.4
	Agree	22	25.6	25.6	100.0
	Strongly agree				
	Total	86	100.0	100.0	

13.2 Retain existing / get more customers

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		4	4.7	4.7	4.7
	Slightly disagree	12	14.0	14.0	18.6
	Slightly agree	50	58.1	58.1	76.7
	Agree	20	23.3	23.3	100.0
	Strongly agree				
	Total	86	100.0	100.0	

13.3 Save money from paying non-compliance fines

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	1.2	1.2	1.2
		2	2.3	2.3	3.5
	Disagree	9	10.5	10.5	14.0
	Slightly disagree	50	58.1	58.1	72.1
	Slightly agree	24	27.9	27.9	100.0
	Agree				
	Strongly agree				
	Total	86	100.0	100.0	

13.4 Better alignment to existing technology

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		2	2.3	2.3	2.3
	Slightly disagree	7	8.1	8.1	10.5
	Slightly agree	58	67.4	67.4	77.9
	Agree	19	22.1	22.1	100.0
	Strongly agree				
	Total	86	100.0	100.0	

13.5 Better security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		3	3.5	3.5	3.5
	Slightly disagree	5	5.8	5.8	9.3
	Slightly agree	55	64.0	64.0	73.3
	Agree	23	26.7	26.7	100.0
	Strongly agree				
	Total	86	100.0	100.0	

13.6 Reduced maintenance cost

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	1.2	1.2	1.2
	Strongly disagree	6	7.0	7.0	8.1
	Slightly disagree	5	5.8	5.8	14.0
	Slightly agree	54	62.8	62.8	76.7
	Agree	20	23.3	23.3	100.0
	Strongly agree				
	Total	86	100.0	100.0	

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
13.1 Maintain a strong reputation	86	5.06	.802	.087
13.2 Retain existing / get more customers	86	5.00	.751	.081
13.3 Save money from paying non-compliance fines	86	5.09	.761	.082
13.4 Better alignment to existing technology	86	5.09	.625	.067
13.5 Better security	86	5.14	.671	.072
13.6 Reduced maintenance cost	86	4.99	.874	.094

One-Sample Test

	Test Value = 3.5	
		95% Confidence Interval of the Difference

	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
13.1 Maintain a strong reputation	18.011	85	.000	1.558	1.39	1.73
13.2 Retain existing / get more customers	18.511	85	.000	1.500	1.34	1.66
13.3 Save money from paying non-compliance fines	19.407	85	.000	1.593	1.43	1.76
13.4 Better alignment to existing technology	23.618	85	.000	1.593	1.46	1.73
13.5 Better security	22.643	85	.000	1.640	1.50	1.78
13.6 Reduced maintenance cost	15.785	85	.000	1.488	1.30	1.68

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
BEN	86	5.0620	.66078	.07125

One-Sample Test

	Test Value = 3.5					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
BEN	21.922	85	.000	1.56202	1.4203	1.7037

14.1 Lack of support from top management in the form of funding

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		13	15.1	15.1	15.1
		12	14.0	14.0	29.1
	Strongly disagree	12	14.0	14.0	43.0
	Disagree	18	20.9	20.9	64.0
	Slightly disagree	23	26.7	26.7	90.7
	Slightly agree	8	9.3	9.3	100.0
	Agree				
	Strongly agree				
	Total	86	100.0	100.0	

14.2 Lack of support from top management in the form of human resources

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		11	12.8	12.8	12.8
	Strongly disagree	14	16.3	16.3	29.1
	Disagree	11	12.8	12.8	41.9
	Slightly disagree				

	Slightly agree	21	24.4	24.4	66.3
	Agree	21	24.4	24.4	90.7
	Strongly agree	8	9.3	9.3	100.0
	Total	86	100.0	100.0	

14.3 The POPIA document is not comprehensive and does not provide guidance for implementation.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		12	14.0	14.0	14.0
		13	15.1	15.1	29.1
	Strongly disagree	3	3.5	3.5	32.6
	Disagree	15	17.4	17.4	50.0
	Slightly disagree	16	18.6	18.6	68.6
	Slightly agree	27	31.4	31.4	100.0
	Agree	86	100.0	100.0	
	Strongly agree				
	Total				

14.4 The government does not provide organisations with support to implement the POPIA

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		3	3.5	3.5	3.5
	Strongly disagree	11	12.8	12.8	16.3
	Disagree	10	11.6	11.6	27.9
	Slightly disagree	9	10.5	10.5	38.4
	Slightly agree	13	15.1	15.1	53.5
	Agree	40	46.5	46.5	100.0
	Strongly agree				
	Total				

	86	100.0	100.0	

14.5 The organisation does not know where to start when implementing the POPIA

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		15	17.4	17.4	17.4
		13	15.1	15.1	32.6
	Strongly disagree	3	3.5	3.5	36.0
	Disagree	7	8.1	8.1	44.2
	Slightly disagree	20	23.3	23.3	67.4
	Slightly agree	28	32.6	32.6	100.0
	Agree				
	Strongly agree				
	Total	86	100.0	100.0	

14.6 Dealing with data breaches

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		7	8.1	8.1	8.1
		10	11.6	11.6	19.8
	Strongly disagree	5	5.8	5.8	25.6
	Disagree	26	30.2	30.2	55.8
	Slightly disagree	20	23.3	23.3	79.1
	Slightly agree	18	20.9	20.9	100.0
	Agree				
	Strongly agree				
	Total	86	100.0	100.0	

14.7 Getting consent to use data

	Frequency	Percent	Valid Percent	Cumulative Percent

Valid	Strongly disagree	3	3.5	3.5	3.5
	Disagree	12	14.0	14.0	17.4
	Slightly disagree	7	8.1	8.1	25.6
	Slightly agree	20	23.3	23.3	48.8
	Agree	26	30.2	30.2	79.1
	Strongly agree	18	20.9	20.9	100.0
	Total	86	100.0	100.0	

14.8 Adapting to new requirements

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		8	9.3	9.3	9.3
		12	14.0	14.0	23.3
	Strongly disagree	6	7.0	7.0	30.2
	Disagree	18	20.9	20.9	51.2
	Slightly disagree	27	31.4	31.4	82.6
	Slightly agree	15	17.4	17.4	100.0
	Agree	86	100.0	100.0	
	Strongly agree				
	Total				

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
14.1 Lack of support from top management in the form of funding	86	3.58	1.598	.172
14.2 Lack of support from top management in the form of human resources	86	3.59	1.552	.167

14.3 The POPIA document is not comprehensive and does not provide guidance for implementation.	86	4.06	1.837	.198
14.4 The government does not provide organisations with support to implement the POPIA	86	4.60	1.618	.174
14.5 The organisation does not know where to start when implementing the POPIA	86	4.02	1.946	.210
14.6 Dealing with data breaches	86	4.12	1.529	.165
14.7 Getting consent to use data	86	4.26	1.432	.154
14.8 Adapting to new requirements	86	4.03	1.583	.171

One-Sample Test

	Test Value = 3.5					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
14.1 Lack of support from top management in the form of funding	.472	85	.638	.081	-.26	.42
14.2 Lack of support from top management in the form of human resources	.556	85	.580	.093	-.24	.43
14.3 The POPIA document is not comprehensive and does not provide guidance for implementation.	2.818	85	.006	.558	.16	.95
14.4 The government does not provide organisations with support to implement the POPIA	6.331	85	.000	1.105	.76	1.45

14.5 The organisation does not know where to start when implementing the POPIA	2.493	85	.015	.523	.11	.94
14.6 Dealing with data breaches	3.737	85	.000	.616	.29	.94
14.7 Getting consent to use data	4.894	85	.000	.756 .535	.45	1.06
14.8 Adapting to new requirements	3.134	85	.002		.20	.87

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
ORG	86	3.8140	1.60385	.17295
EXT	86	4.2529	1.36365	.14705

One-Sample Test

	Test Value = 3.5					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
ORG	1.815		.073	.31395		.6578
EXT	5.120	85 85	.000	.75291	-.0299 .4605	1.0453

Annexure 3

Questionnaire

Answer EVERY question by selecting the response option that best applies to you

Section A Demographics

1 Your gender?

Male	Female

2 Your age?

Under 20 years	20 – 25 years	26 – 30 years	31 -35 years	36 – 40 years	41 – 45 years	Over 45 years

3 Indicate which of the following functions you perform in your organisation/business for the e-commerce system. (**Tick all that apply**)

FUNCTIONS	Yes	No
3.1 Information security implementation		
3.2 Software developer		
3.3 Project manager		
3.4 Database administrator / designer		

4 How long have you worked in the field?

Less than 1 year	1 – <2 years	2 – <3 years	3 – 4 years	More than 4 years

5 Indicate your awareness and knowledge of the POPIA legislation? (Select **ONE** option only)

I have not heard of the POPIA legislation	I have heard of POPIA but don't know anything about it	I have heard of POPIA and know a little about it	I have heard of POPIA and know a lot about it

Section B Implementing POPIA

1 Indicate which of the following information security best practices and frameworks are used in your organisation to assist in implementing the 7th condition of the POPIA

	Yes	No

1.1 COBIT 5		
1.2 IS0 27001 / 27002		
1.3 GAAP		
1.4 NIST SP 800		

2 Indicate if you use the following to technically protect the information resource managed by your organisation

	Yes	No
2.1 Encryption		
2.2 Web Application Firewall		
2.3 Physical security		
2.4 Database audits		

3 Indicate your level of agreement with the following statements.

	Strongly disagree	Disagree	Slightly disagree	Slightly agree	Agree	Strongly agree
3.1 The company provides me with adequate Information Security Training awareness						
3.2 Top management understands the contents of the POPIA legislation						

4 Indicate whether you measure the effectiveness of your information security awareness training using the following methods

	Yes	No
4.1 Questionnaires		
4.2 Interviews		

5 Do you ALWAYS get consent from your customers to store and process their data?

Yes	No

6 Indicate whether you use the following to ensure that users of your site are aware of how their data will be stored and processed

	Yes	No
6.1 Privacy policy statement on website		
6.2 Terms and conditions statement on website		
6.3 Other		

If you responded 'OTHER' please specify what other method, you use

_____

7 Indicate if your organisation takes any of the following actions to ensure that customers are informed when there is a data breach.

	Yes	No
7.1 Nothing		
7.2 SMS / Text		
7.3 Call		
7.4 Put an announcement on the website		
7.5 Other action		

If you responded 'OTHER' please specify what other method, you use.

_____

8 Which of the following risks do you encounter most often in your business? (Select ONE option only)

Database hack	Denial-of-service attack	Theft of customer payment while in transit details

9 Indicate which of the following controls you apply to ensure that your information resource is accessed by legitimate people

	Yes	No
9.1 Access control levels		
9.2 Verification process		
9.3 Other control		

If you responded 'OTHER' please specify what other method, you use

_____

10 How frequently does your organisation update its risk analysis list? (Select ONE option only)

At least every 3 months	Every 3 – <6 months	Every 6 – <9 months	Every 9 – 12 Months	Less often than every 12 months	Never

11. Indicate your level of agreement with the following statements

	Strongly disagree	Disagree	Slightly disagree	Slightly agree	Agree	Strongly agree
11.1 Management provides adequate support to implement the POPIA 7TH condition						
11.2 Management provides a budget to implement compliance measures						
11.3 Management employs an outside company to oversee certain aspects of the POPIA task						
11.4. Management audits our POPIA compliance						
11.5 Management ensures that third party organisations are also compliant						
11.6. Management provides us with up-to-date training so that we know what is right or wrong						
11.7 Management has developed policies to drive the POPIA in the organisation						

12 Indicate your level of agreement that the following are consequences you face if you disregard POPIA.

	Strongly disagree	Disagree	Slightly disagree	Slightly agree	Agree	Strongly agree
12.1 Reputational Damage						
12.2 Imprisonment						
12.3 Loss of customer confidence						
12.4 Heavy fines						

13 Indicate your level of agreement that the following are benefits that the organisation can enjoy when implementing POPIA:

	Strongly disagree	Disagree	Slightly disagree	Slightly agree	Agree	Strongly agree
13.1 Maintain a strong reputation						
13.2 Retain existing / get more customers						
13.3 Save money from paying noncompliance fines						
13.4 Better alignment to existing technology						
13.5 Better security						
13.6 Reduced maintenance cost						

14 Indicate your level of agreement that the following are challenges you encounter when implementing POPIA:

	Strongly disagree	Disagree	Slightly disagree	Slightly agree	Agree	Strongly agree
14.1 Lack of support from top management in the form of funding						
14.2 Lack of support from top management in the form of human resources						
14.3 The POPIA document is not						
comprehensive and does not provide guidance for implementation.						
14.4 The government does not provide organisations with support to implement the POPIA.						
14.5 The organisation does not know where to start when implementing the POPIA						
14.6 Dealing with data breaches						
14.7 Getting consent to use data						
14.8 Adapting to new requirements						

END OF QUESTIONNAIRE

4

Ethical clearance

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

30 October 2020

Mr Lehlohonolo Itumeleng Moraka (219095366)
School Of Man Info Tech &Gov
Westville Campus

Dear Mr Moraka,

Protocol reference number: HSSREC/00001947/2020
Project title: A framework for the Protection of Personal Information Act compliance in the e-commerce IT sector
Degree: Masters

Approval Notification – Expedited Application

This letter serves to notify you that your application received on 19 August 2020 in connection with the above, was reviewed by the Humanities and Social Sciences Research Ethics Committee (HSSREC) and the protocol has been granted **FULL APPROVAL** on the following condition:

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment/modification prior to its implementation. In case you have further queries, please quote the above reference number. PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

This approval is valid until 30 October 2021.
To ensure uninterrupted approval of this study beyond the approval expiry date, a progress report must be submitted to the Research Office on the appropriate form 2 - 3 months before the expiry date. A close-out report to be submitted when study is finished.

All research conducted during the COVID-19 period must adhere to the national and UKZN guidelines.

HSSREC is registered with the South African National Research Ethics Council (REC-040414-040).

Yours sincerely,

[redacted]

5

Gate keepers consent letter

17 July 2020

Itumeleng Moraka
Masters degree student, UKZN
Request for Permission to Conduct Research

Dear Director

My name is Itumeleng Moraka, a Masters degree student at the University of Kwazulu-Natal. The research I wish to conduct for my Masters dissertation involves developing: A framework for the Protection of Personal Information Act compliance in the e-commerce IT sector.

I am hereby seeking your consent to distribute a survey and use the survey outcome as part of my research project.

I have provided you with a copy of my proposal which includes copies of the data collection tools and consent and/ or assent forms to be used in the research process, as well as a copy of the approval letter which I received from the Institutional Research Ethics Committee (IREC).

If you require any further information, please do not hesitate to contact me on: 082 642 9787 or email me on: 219095366@stu.ukzn.ac.za. Thank you for your time and consideration in this matter.

Yours sincerely,
Itumeleng Moraka University of Kwazulu-Natal

6

Language editors' certificate

ETHEL ROSS

English language editing and proofreading

20 August 2021

To whomever it may concern:

This letter serves to confirm that I worked as the proofreader and language editor on Lehlohonolo Itumeleng Moraka's dissertation:

THE COMPLIANCE FRAMEWORK FOR THE 7TH POPIA CONDITION IN THE SME ICT SECTOR

In no way did I change the content.

Yours faithfully

[redacted]

Ethel Ross (BA Hons; H Dip Ed)

Email: clanross1@icon.co.za Tel: 083 954 5412