

**Factors affecting information security compliance among SMEs in
Cape Town.**

Felencia Linthea Lawrence

Student number: 3329196

A thesis submitted in fulfilment of the requirements for the degree of Master of Commerce in
Information Systems in the Department of Information Systems
Faculty of the Economic and Management Sciences University of the Western Cape

Supervisor: Professor Osden Jokonya

November 2022


PLAGIARISM DECLARATION

Declaration

I, Felencia Linthea Lawrence declare that “*Factors affecting information security compliance among Small-medium enterprises (SMEs) in Cape town*” is my own work, that it has not been submitted for any degree or examination in any other university, and that all the sources I have used or quoted have been indicated and acknowledged by complete references. The plagiarism similarity index can be found in Appendix F.

Full name: Felencia Linthea Lawrence

Date: November 2022

Signature:  _____

ABSTRACT

Factors affecting information security compliance among SMEs in Cape Town.

F.L Lawrence

November 2022

Master of Commerce in Information Systems, Department of Information Systems, Faculty of Economic and Management Sciences, University of the Western Cape

Small and medium enterprises are depending on the use of IT systems to compete and participate in the South African economy and also to improve the efficiency of their service delivery. Using IT systems in their business has increased risks and hazards regarding information security. Even though information security has been around for a while and several research studies have been conducted on the topic, it is still unclear how SMEs comply with the standards and regulations that are associated with it. The study aimed to fill this gap by examining the information security phenomenon from the point of view of South African SMEs. The purpose of this study was to investigate the factors that influence the adoption of information security compliance by SMEs. Following a survey design together with a quantitative research approach, the collection of survey questionnaires was used as a means of data collection. In addition, the data obtained from the surveys collected was analysed using a quantitative data analysis process. The study revealed several technological, organizational, and environmental factors that influence the organization's readiness to be compliant with information security policies as well as South African regulations and global standards. The results revealed a positive relationship between these factors that significantly impact the organization. The study contributes towards improved information security management guidance and compliance for small to medium businesses as well as greater accountability, integrity, and governance among employees. Practical recommendations were also provided to SMEs for effective IS compliance. The suggestion for further research should consider psychological elements to ensure information security compliance in organizations. Additional categories of characteristics that influence management and staff adherence to information security standards should also be thoroughly studied. The utilization of alternate research techniques for data collection is also a further perspective for future studies.

Keywords: Information security compliance, policies, standards, regulations, Small-Medium Enterprises, Cape Town, South Africa, Technological, Organizational, Environmental.

ACKNOWLEDGEMENTS

"So do not fear, for I am with you; do not be dismayed, for I am your God. I will strengthen you and help you; I will uphold you with my righteous right hand". (Isaiah 41:10).



"Moenie bang wees nie, Ek is by jou, moenie bekommerd wees nie, Ek is jou God. Ek versterk jou, Ek help jou, Ek hou jou vas, met my eie hand red Ek jou". (Jesaja 41:10).



First, I would like to give praise to God the Almighty for giving me the strength and courage to complete my thesis successfully. Secondly, would like to thank my supervisor Prof. Osden Jokonya for his countless advice and guidance during the completion of my thesis. All his effort and time during this journey were highly appreciated. Then, would like to show my appreciation to all the mentors at the Division for Post-Graduate Studies (DPGS) who were always available to assist me when I needed advice with my research. Lastly, I would like to thank all my family members for always being patient and understanding with me during this journey.

LIST OF TABLES

Table 1: Definition of small and medium enterprises in South Africa (Source: Fatoki, 2011).....	3
Table 2: Small to Medium categories (Source: Olawale & Garwe, 2010).....	9
Table 3: The eight principles of the POPI Act (Source: POPI Act 4, 2013).....	28
Table 4: Definitions of key research paradigms (Sources: Saunders, Lewis, & Thornhill, 2019)....	42
Table 5: Deduction, induction, and abduction (Source: Saunders, Lewis, & Thornhill, 2019).....	43
Table 6: Weekly timeline of survey strategy.....	47
Table 7: Primary data vs Secondary data (Source: Ajayi, 2017).....	50
Table 8: Survey distribution and collection by organization type.....	59
Table 9: Likert scale analysis.....	64
Table 10: Reliability statistics of Technological-Organizational-Environmental Factors.....	65
Table 11: Validity of technological factors.....	66
Table 12: Component matrix of technological factors.....	66
Table 13: Validity of Organizational factors.....	67
Table 14: Component matrix of organizational factors.....	67
Table 15: Validity of Environmental factors.....	68
Table 16: Component matrix of Environmental factors.....	68
Table 17: Test for normality of data.....	69
Table 18: Technological factors.....	71
Table 19: Correlation matrix of the technological factors.....	71
Table 20: Organizational factors.....	72
Table 21: Correlation matrix of organizational factors.....	73
Table 22: Environmental factors.....	74
Table 23: Correlation matrix of organizational factors.....	75
Table 24: Correlation matrix.....	71
Table 25: Relationship between job position and experience.....	75
Table 26: Regression model summary.....	77
Table 27: Analysis of variance.....	77
Table 28: Regression Coefficients.....	78

LIST OF FIGURES

Figure 1: Components of Information security (Source: Whitman & Mattord, 2011)	16
Figure 2: The information security triad (Source: Nikander, Manninen, & Laajalahti, 2020)	17
Figure 3: Security controls (Source: Cyber Security Framework, 2018)	21
Figure 4: King IV principles (Source: Ferguson, 2019)	24
Figure 5: Identified security and privacy challenges (Source: Salleh & Janczewska, 2016)	34
Figure 6: Research onion (Source: Saunders, Lewis, & Thornhill, 2019).....	41
Figure 7: Methodological choice (Source: Saunders, Lewis & Thornhill, 2016, p.167).....	45
Figure 8: Respondent's gender	60
Figure 9: Length at company	61
Figure 10: Respondent's job position	62
Figure 11: Organization type	63
Figure 12: Scatterplot of data.....	76

LIST OF ABBREVIATIONS

Abbreviation:	Full term:
ATM	Automated Teller Machine
BD	Big Data
CIA	Confidentiality-Integrity-Availability
CPT	Cape Town
ECT	Electronic Communications and Transaction Act
Email	Electronic Mail
GDP	Gross Domestic Product
ICT	Information and Communication Technology
InfoSec	Information Security
IS	Information Systems
ISP	Information Security Policy
IT	Information Technology
NCPF	National Cybersecurity Policy Framework
NSB	National Small Business Act
POPIA	Protection of Personal Information Act
RSA	Republic of South Africa
SA	South Africa
SMEs	Small-Medium Enterprises
SMME	Small Medium and Micro-Enterprise
SPSS	Statistical Package for the Social Sciences
TOE	Technological-Organizational-Environmental
WC	Western Cape

TABLE OF CONTENT

PLAGIARISM DECLARATION	i
ABSTRACT	ii
ACKNOWLEDGEMENTS	iii
LIST OF TABLES	iv
LIST OF FIGURES	v
LIST OF ABBREVIATIONS	vi
TABLE OF CONTENT	vii
Chapter 1: Introduction	1
1.1 Introduction and research background	1
1.2 Research problem	4
1.3 Main research questions and sub-questions	5
1.4 Research aims.....	5
1.5 Research objectives	5
1.6 Research methodology	6
1.7 Significance of study	6
1.8 Thesis outline	6
1.8.1 Chapter 1: Introduction	6
1.8.2 Chapter 2: Literature review	7
1.8.3 Chapter 3: Research Methodology.....	7
1.8.4 Chapter 4: Interpretation and discussion of findings	7
1.8.5 Chapter 5: Conclusion.....	7
1.9 Chapter Summary.....	7
Chapter 2: Literature review	8
2.1 Introduction	8
2.2 Overview of Small-medium enterprises (SMEs)	8

2.2.1	Definition of SMEs	8
2.2.2	The role of SMEs in South Africa	9
2.2.3	Challenges of SMEs.....	10
2.3	Information conceptualization.....	12
2.3.1	Defining information	12
2.3.2	The importance of information	13
2.4	Overview of Information security (InfoSec).....	14
2.4.1	Defining Information security (InfoSec)	14
2.4.2	Information security principles.....	16
2.4.3	Information security policies (ISP).....	18
2.4.4	Information security standards	19
2.4.5	Information security controls.....	20
2.4.6	Information security compliance.....	22
2.5	Information security governance.....	23
2.5.1	King IV.....	23
2.5.2	Electronic Communications and Transactions Act (ECT).....	25
2.5.3	Protection of Personal Information (POPI) Act	26
2.6	Information security theories and frameworks.....	30
2.6.1	Institutional theory.....	30
2.6.2	The National Cybersecurity Policy Framework (NCPF).....	32
2.6.3	Technological-Organizational-Environmental framework (TOE)	33
2.7	Chapter Summary.....	39
Chapter 3: Research Methodology.....		40
3.1	Introduction	40
3.1.1	The research onion framework	40
3.1.2	The rationale for using the research onion	41
3.2	Research Philosophy: Positivism	42
3.3	Research Approach: Deduction, Inductions, and Abduction	43
3.4	Methodological Choice: Quantitative research design.....	44
3.4.1	Unit of analysis	45
3.5	Research Strategy: Survey.....	46
3.6	Research time horizon: Cross-sectional	47

3.7	Data Collection.....	48
3.7.1	Population	48
3.7.2	Primary data	49
3.7.3	Instrument development: Survey.....	50
3.7.4	Survey questionnaire: Validity and Reliability	51
3.7.5	Reliability	53
3.7.6	Disposal of data	53
3.8	Data Analysis	54
3.8.1	Quantitative data.....	54
3.8.2	Statistical analysis.....	54
3.8.3	The quantitative data analysis process	54
3.9	Ethical considerations.....	55
3.10	Chapter Summary	56
	Chapter 4: Interpretation and discussion of findings.....	58
4.1	Introduction	58
4.2	Survey response.....	59
4.3	Biographic information of the respondents	59
4.3.1	Gender of respondents.....	60
4.3.2	Length at company	60
4.3.3	Job position.....	61
4.3.4	Organization type	62
4.4	Characteristics of the instrument development	63
4.4.1	Likert scale analysis	63
4.4.2	Reliability (Internal consistency - Cronbach's alpha).....	64
4.4.3	Validity and factor analysis.....	65
4.4.4	Test for normality	69
4.5	Factors affecting the adoption of information security compliance.....	70
4.5.1	Technological factors.....	70
4.5.2	Organizational factors	72
4.5.3	Environmental factors	74
4.6	The relationship between the T-O-E factors	76
4.7	The relationship between job position and experience	74

4.8	The successful adoption of InfoSec compliance	75
4.8.1	Normality test.....	75
4.8.2	Simple linear regression	76
4.9	Practical recommendations for SMEs	78
4.9.1	Technological compatibility.....	78
4.9.2	Technological complexity	78
4.9.3	Existing technology.....	78
4.9.4	Organizational learning culture	79
4.9.5	Information security awareness.....	79
4.9.6	Top management support.....	79
4.9.7	Policies and standards	79
4.9.8	Security and privacy compliance	80
4.9.9	Privacy and security regulations.....	80
4.9.10	Risks in outsourcing.....	80
4.10	Chapter Summary	81
Chapter 5: Conclusion & Recommendation.....		83
5.1	Introduction	83
5.2	Main research question and sub-questions	83
5.3	Re-examine the aims and objectives of the study	84
5.4	Summary of the research study	84
5.4.1	Chapter 1	84
5.4.2	Chapter 2	85
5.4.3	Chapter 3	85
5.4.4	Chapter 4	86
5.5	Summary of the results.....	87
5.5.1	Survey response	87
5.5.2	Biographic information of respondents	87
5.5.3	Characteristics of instrument development.....	87
5.5.4	Technological factors.....	88
5.5.5	Organizational factors	89
5.5.6	Environmental factors	89
5.5.7	The relationship between the T-O-E factors	90
5.5.8	The relationship between job position and experience with InfoSec Compliance	90

5.5.9	The successful adoption of InfoSec Compliance	90
5.5.10	Practical recommendations for SMEs	91
5.6	Critical evaluation of the research objectives.....	91
5.6.1	Objective 1: To determine the technological factors impacting the adoption of information security compliance among SMEs	92
5.6.2	Objective 2: To determine the organizational factors influencing the adoption of information security compliance among SMEs	92
5.6.3	Objective 3: To determine the environmental factors affecting the adoption of information security compliance among SMEs	92
5.6.4	Objective 4: To reach conclusions drawn from the research study to make practical recommendations to SMEs.	93
5.7	Limitations of study.....	93
5.8	Contribution of research.....	93
5.9	Suggestions for future research	94
5.10	Conclusion of study	94
References		95
 APPENDIX A: Ethical Clearance Certificate		113
APPENDIX B: Participation information sheet for SMEs in Cape Town		114
APPENDIX C: Consent form for SMEs in Cape Town		117
APPENDIX D: Information Security survey for SMEs in Cape Town.....		119
APPENDIX E: Mean scores and Standard deviation.....		126
APPENDIX F: Plagiarism Similarity Index.....		129

Chapter 1: Introduction

1.1 Introduction and research background

Information is considered a vital asset in organizations today as it influences organizational culture. According to Belan (2015), information becomes one of the company's most crucial competitive advantages and a valuable product. (Khouri, 2009), refers to information as one of the most valuable resources that businesses possess. As a result, it requires protection that is commensurate with its value. Information and knowledge are essential tools for enhancing how small and medium-sized businesses (SMEs) internationalize (Costa, Soares, & De Sousa, 2016). A more rational decision-making process is enabled by information that is more explicit and comprehensive, but the ability of the decision-maker to recognize, seek out, and digest information is also crucial for making more efficient internationalization decisions (Hsu, Chen, & Cheng, 2013). Information and knowledge are seen as essential for managing global complexity and ambiguity, minimizing risks, and fostering awareness of international market opportunities (Zhou, Wu, & Luo, 2007).

Information security is crucial to the management of businesses. According to Wang & Wendy (2019), “information security considers the security of computer systems to protect them against disclosure, subjective modification, unauthorized access, harassment, or destruction aiming to ensure integrity, confidentiality, and availability of information”. It protects one of its most important resources, data, and information, and ensures its confidentiality, privacy, integrity, and availability (Antunes, Maximiano, Gomes, & Pinto, 2021). Due to their size, localized scope, financial resources, and perceived blind spot in information security and cybersecurity management, small and medium-sized businesses (SMEs) are often overlooked (Antunes, Maximiano, Gomes, & Pinto, 2021). However, Ikeda, Marshall, & Zaharchuk (2019), argues that businesses are more aware of cybersecurity and information security management since it is believed that these are important issues for survival and competition in international marketplaces. Management boards are increasingly aware of the need to secure data and information, but at the same time, cyberattacks are on the rise, as reported by international cybersecurity institutions, and awareness of the need to implement countermeasures has significantly increased (Al-Sartawi, 2020).

With an increase in attacks and security incidents, information security and data protection are becoming increasingly important on a global scale (Bolek, Látečková, Romanová, & Korček, 2016). Organizational security rules are not updated to reflect technological advancements because it is still difficult to foresee future developments (Von Schomberg, 2016). Numerous guidelines and standards

encourage businesses to increase their spending on information security (Srinivas, Das, & Kumar, 2019). However, little is known about how SMEs employ security measures, how they view the risk of cybercrime, and how they have dealt with cyberattacks (Huaman, von Skarczinski, & Stransky, 2021). Government regulations and standards require enterprises to make an effort to preserve information due to the rise in cyber risks and the loss of capital (AlKalbani, Deng, Kam, & Zhang, 2017). The authors further state that the effort of organizations to protect information is mandated by government regulations and standards due to the increase in cyber threats and the loss of capital.

Small and medium-sized businesses (SMEs) are important to the economy since they account for a sizable portion of the wealth generated globally (Nistotskaya, Charron, & Lapuente, 2015). However, their inherent qualities namely, their small size, the fact that they are based on well-known and established structures, and their resource typology put them in a second position in terms of cybersecurity awareness and information security (Kertysova, Frinking, & van den Dool, 2018). Even though many SMEs may only have a basic IT infrastructure to fend off cyberattacks, they can take action, in the beginning, to gradually raise their level of security (Saleem, Adebisi, Ande, & Hammoudeh, 2017). Therefore, organizations must make sure that their operational procedures, workplace guidelines, and employee behaviour enable them to reduce and even eliminate some of the risks associated with their information systems and IT infrastructures (Bell, 2017).

Recent years have seen an increase in the number of cyberattacks that target small and medium-sized businesses (SMEs) (Huaman, von Skarczinski, & Stransky, 2021). The authors also claim that SMEs frequently lack the knowledge and funding necessary to implement comprehensive information security procedures. IT and IS infrastructure are less relevant to SMEs given their total employees, annual turnover, and asset value (see Table 1) since the company lacks the resources or personnel to keep up with new technological concepts (Rahmana, Yaacobb, & Radzic, 2016). Small and medium-sized businesses may lack the knowledge and resources necessary to effectively defend themselves against assaults, while major firms frequently have substantial resources and specialized security teams available (Abraham, Chatterjee, & Sims, 2019). However, because information systems are becoming more vulnerable, cyber security is now seen as a concern that affects both public and private enterprises (Abbott, McClain, & Anderson, 2015). This is especially true for small and medium-sized businesses (SMEs), who sometimes lack the funding necessary to purchase and deploy cyber security measures in their operations (Sulayman, Urquhart, Mendes, & Seide, 2012).

Table 1: Definition of small and medium enterprises in South Africa (Source: Fatoki, 2011)

<i>Sector</i>	<i>Total full-time employees (Less than)</i>	<i>Total annual turnover (Less than)</i>	<i>Total gross asset value (Less than)</i>
Manufacturing	Medium	200	R40m
	Small	50	R10m
Retail	Medium	120	R30m
	Small	50	R15m
Wholesale	Medium	120	R50m
	Small	50	R25m
Business services	Medium	120	R20m
	Small	50	R10m

Organizations now face unprecedented challenges in securing their sensitive information due to an increased reliance on information technologies (Gupta, 2011). All of which directly affect corporate accountability decreased credibility, and financial loss. Information security is now crucial in many firms as a result (AlKalbani, Deng, & Kam, 2016). Information security compliance refers to the application of information security standards and policies for protecting information in organizations (AlKalbani, et al., 2014; Von Solms, 2005). Compliance with information security regulations ensures that firms' information security procedures can work effectively together to secure sensitive data (Ifinedo, 2014). It complies with security requirements, boosting stakeholder confidence and trust in organizations. Information security compliance is therefore widely recognized as a successful method for guaranteeing data security in organizations (Herath & Rao, 2009).

To properly protect the organization's information and data, information security compliance is becoming more crucial (Boss & Kirsch, 2007; Von Solms, 2001). On the other side, implementing a compliance strategy for information security is challenging and complex. This is because it necessitates (a) the implementation of efficient information security processes and mechanisms, (b) meeting the legal and security needs of various organizations and their stakeholders, and (c) maintaining the faith and trust of both employees and stakeholders (Steinbart, Raschke, Gal, & Dilla, 2012). The objective of this study was to identify the factors that create challenges for SMEs in Cape Town related to Information Security Compliance adoption. To accomplish this, data collected

through online surveys were analyzed and practical recommendations for effective information security policies and standards were proposed.

1.2 Research problem

Organizations value information and data because it advances business processes. Although SMEs hold sensitive data about their employees, customers, and business partners, they tend to have limited resources to acquire and implement security mechanisms in their organizations and do not have a dedicated IT management department that can handle these responsibilities (Sulayman, Urquhart, Mendes, & Seide, 2012; Leung, 2012). Therefore, information security policies and standards are crucial because it reduces the potential threat of data breaches and cyber-attacks on IT systems. The complexities of information security required in running small-medium enterprises (SMEs) are often challenging compared to large enterprises (Kabanda, Tanner, & Kent, 2018). As the importance of information security has grown, organizations have been under pressure to comply with information security policies and standards regarding the protection of company data (AlKalbani, Deng, Kam, & Zhang, 2017).

In light of the above discussion, it has been discovered that SMEs pay little attention to security issues, and as a result, findings on ICT security in SMEs are typically negative (Nycz, Martin, & Polkowski, 2015). According to Kent, Tanner, & Kabanda (2016), SME attitudes about information security are difficult to predict mainly because of three reasons:

- SMEs prefer to focus on regulatory compliance rather than protecting their organization's security.
- Restricted resources had a negative attitude toward security because there seems to be no immediate return on investment.
- The belief is that SMEs, particularly start-ups, will not become a target for security attacks.

The research aimed to investigate and identify what factors are preventing SMEs from adopting information security in their organization by determining the factors from a technological, organizational, and environmental perspective.

1.3 Main research questions and sub-questions

Main research question:

What are the factors affecting the adoption of information security compliance among SMEs?

Sub-questions:

1. What technological factors are impacting SMEs' adoption of information security compliance?
2. What organizational factors are influencing SMEs' adoption of information security compliance?
3. What environmental factors affect the adoption of information security compliance by SMEs?
4. What recommendations can be made to assist SMEs in meeting their information security compliance obligations?

1.4 Research aims

This study aimed to assess the importance of information security in small-medium enterprises by identifying the factors that contribute to information security adoption challenges. The results of this study contribute towards improved security management systems for small to medium businesses as well as greater accountability, integrity, and governance among employees. Practical recommendations were also provided to SMEs for effective IS compliance in this study.

1.5 Research objectives

Based on the evidence presented in section 1.2. The following aims and objectives were considered for this study:

- To determine the technological factors impacting the adoption of information security compliance among SMEs.
- To determine the organizational factors influencing the adoption of information security compliance among SMEs.
- To determine the environmental factors affecting the adoption of information security compliance among SMEs.
- To make recommendations on ways to improve the adoption of information security compliance among SMEs.

1.6 Research methodology

The research methodology for this study was guided by the research onion structure that was first developed in 2007 by Saunders, Lewis, and Thornhill. In an illustration of the latest research onion (2019), the authors presented the different stages when developing knowledge during a research study. This framework was chosen for this study because it improves the researcher's comprehension of the many stages associated with various techniques of data gathering and provides illustrations for methodological investigations. The research onion has several advantages, including the fact that it can be effectively adapted to different models and it is a useful tool for thinking holistically about the methodology used.

1.7 Significance of study

Information has become one of the most valuable assets for individuals, organizations, and corporations. Currently, businesses prioritize the security of their information, so information security is always in the news (Niranjanamurthy & Chahar, 2013). However, to attain a high degree of information security, a company must guarantee cooperation on all fronts, including the use of information, which entails integrating all parties both inside and outside the company (Fernandes, Soares, & Gomes, 2014). There is no consensus in the industry regarding what constitutes efficient information security for small and medium-sized businesses (Chen, Chiang, & Storey, 2012). To ensure information security systems are designed and implemented effectively, the highest level of management must be involved in all stages of the process (Fernandez & Rainey, 2017). It is therefore imperative to maintain information security compliance as part of everyday duties, and qualified personnel is essential.

1.8 Thesis outline

The study is broken down into five sections. Below is an outline of each chapter.

1.8.1 Chapter 1: Introduction

Chapter 1 presents the introduction of the research study. It gives a brief background to the research study followed by the research problem. This is followed by the research problem, research questions, the research aims, research objectives, research methodology, and lastly the significance of the study.

1.8.2 Chapter 2: Literature review

Chapter 2 provides an in-depth literature review, where the author investigated previous scientific research in Information systems from scholars and experts. The chapter concludes with framing information security compliance with the TOE framework by discussing technological, organizational, and environmental behaviours.

1.8.3 Chapter 3: Research Methodology

Chapter 3 covers the research methodology and methods used in this study. It gives an overview of the research design, research paradigms, research philosophies, and research approach. It also describes the research strategy, data collection, and data analysis followed by the ethical considerations for this study.

1.8.4 Chapter 4: Interpretation and discussion of findings

Chapter 4 presents the interpretation and discussion of the findings of this descriptive study by starting with the background of the respondents used in this study. Then a presentation of the overall analysis of the results given of the research study that was conducted. The chapter discusses trends and patterns based on the analysis and will conclude the chapter with a summary of positive and negative results.

1.8.5 Chapter 5: Conclusion

Chapter 5 presents the conclusion of this study by discussing the research aims and objectives. This is followed by the research questions, results, implications, limitations, and contribution of this study. Then the study is concluded with recommendations for future studies.

1.9 Chapter Summary

Section 1: the researcher provided an in-depth introduction and research background to the research topic of this study. **Section 2:** The problem statement was presented as SMEs fail to pay attention to information security due to the lack of awareness and adoption challenges. **Section 3:** This was followed by the research primary questions and sub-questions. **Sections 4 & 5:** Also, the research aim was discussed followed by the research objectives. **Section 6:** Furthermore, the research methodology of the study was presented. **Section 7 & 8:** The next section describes the significance of the study followed by the chapter conclusion as the thesis outline. The following chapter covers the literature relevant to the research topic of this study.

Chapter 2: Literature review

2.1 Introduction

The previous chapter presented an introduction to the research, this chapter outlines and discusses a literature review of the research. An academic definition of a literature review is a part of the thesis that references related research and theory (Ridley, 2012). During this process, connections are made between the sources used for research and how they position among these sources. The literature review is outlined as follows.

In section 2.2 of the literature review, a synopsis of small-medium enterprises is presented where the definition of SMEs is discussed, the role of SMEs in South Africa, and the challenges faced by SMEs. Section 2.3 presents the conceptualization of information provided, as accurately as the role and importance of information in a business environment. Section 2.4 discusses information security by definition, exploring information security principles, information security policies, and standards, information security controls, and information security compliance. In section 2.5, the information security governance is presented by looking at three important acts in South Africa named King IV, the Electronic Communications and Transaction Act, and the Protection of Personal Information Act. Lastly, the chapter ends with section 2.6, where information security theories and frameworks are examined by discussing institutional theories, the National Cybersecurity Policy Framework, and the Technological-Organizational-Environmental framework.

2.2 Overview of Small-medium enterprises (SMEs)

Small-medium enterprises (SMEs) are vital to the economy. To explore the study on information security compliance in SMEs, it is imperative to understand and define what is meant by the term Small-medium enterprises and to analyze SMEs. In South Africa, SMEs are defined as companies with fewer than 200 employees, owners who have managerial involvement, and capital assets worth less than R60 to R65 million (Asah, Fatoki, & Rungani, 2015). As a result, it is important to establish the state of information security compliance adoption among SMEs in South Africa, which is also the aim of this study.

2.2.1 Definition of SMEs

In South Africa, SMEs contribute significantly to economic growth and development (Bvuma & Marnewick, 2020). Small to medium businesses promote job creation in an economy that is known

for a high unemployment rate and lacks sustainable improvement in society. These businesses operate in various parts of the country in both rural and urban areas (Snyman, 2012). Rural areas in developing countries benefit immensely from SMEs, which create jobs, and wealth, and ease poverty (Manzoor, Wei, & Sahito, 2021). Various areas in South Africa can greatly benefit from the formation of SMEs. There are a variety of business formations, from formal to informal, including traditional families (Bvuma & Marnewick, 2020).

The definition of small to medium business can be defined by the South African National Business (NSB) amendment Acts of 2003 as well as 2004:

"SMEs as any entity, whether incorporated or registered under any law, which consists mainly of persons carrying on small business concerns in any economic sector, or which has been established to promote the interests of or represent small business concerns, and includes any federation consisting wholly or partly of such association, and also any branch of such organization" (Mahembe, 2011).

According to the NSB Act, South African small businesses can be divided into "survivalists, micros, very small, small and medium businesses", thus the term SMME, which stands for small, medium, and micro enterprises. To take it one step further, Table 2 below illustrates each size of enterprise based on its type, total employees, turnover, and balance sheet estimate. The table below describes small businesses as having 1 to 50 employees with a turnover maximum of R13 million with a balance sheet of R5 million. Also presented in the table are the medium types of businesses with 50 to 200 employees at a turnover of a maximum of R51 million with a balance sheet of R19 million.

Table 2: Small to Medium categories (Source: Olawale & Garwe, 2010)

Type of Firm	Total employees	Turnover	Balance sheet
Small	1-50	R13 million	Max R5 million
Medium	50-200	R51 million	Max R19 million

2.2.2 The role of SMEs in South Africa

In South Africa, SMEs are increasingly dependent on revenue and job creation for economic growth (Ramukumba, 2014). This enables SMEs to grow as a business as well as create growth in the economy. The South African government has laid appropriate foundations aimed at enhancing

the entrepreneurial opportunities of small and medium-sized businesses to reduce pressure on the social security system (Abor & Quartey, 2010). In particular, it emphasizes enterprise assistance programmes for small and medium-sized businesses. Ramukumba (2014), asserts that for South Africa to prosper economically, new SMEs must be created and sustained. "Without the creation of new SMEs, the country may run the risk of economic stagnation" (Ncube & Zondo, 2022).

According to Ramukumba (2014), the role of SMEs in the economy of South Africa is pivotal because of their ability to create jobs, foster economic development, and create jobs, all of which affect the government and the citizens. To achieve growth in their respective industries, they must operate efficiently and run their businesses effectively (Tseng & Johnsen, 2011). More authors describe the role of SMEs as important in local economies by indicating that they contribute a large portion of gross domestic product up to 60% (Assante, Castro, Hamburg, & Martin, 2016); (Rungani & Potgieter, 2018). Also, in industrialized economies, SMEs account for roughly 70% of the labour force, making them a significant source of employment (Senarathna, Wilkin, Warren, & Yeoh, 2018). Emerging economies have lower levels of these statistics. For instance, South African SMEs account for 60% of all employment and roughly 42% of South Africa's GDP (Rungani & Potgieter, 2018).

To further pinpoint the role of SMEs, one important component in addressing South Africa's development problems is the growth of new SMEs (Ruwanza & Shackleton, 2016). According to Snyman (2012), in low-income countries, SMEs and informal enterprises account for more than 60% of GDP and 70% of employment, while in high-income countries, they constitute more than 55% of GDP and more than 65% of employment. Moreover, they account for approximately 70% of the GDP of middle-income nations, as well as 95% of jobs (Muriithi, 2017). A significant portion of the South African economy is dominated by SMEs, accounting for 52 to 56 percent of the GDP and 56 percent of all private sector jobs (Snyman, 2014). Therefore, it is considered that SMEs are one of the main contributors to the South African Growth Development Product (GDP).

2.2.3 Challenges of SMEs

According to Ramukumba (2014), South Africa's formal and public sectors struggle to employ the country's rising labor force. As a result, more attention is being paid to entrepreneurship, the start-up of new businesses, and their ability to stimulate economic growth and generate jobs. Despite the highlighted benefits of new SMEs, South Africa has one of the highest rates of failure globally. About 75% of newly formed SMEs fail to grow into successful companies (Zvitambo & Chazireni, 2019). Ayandibu & Houghton (2017), claim that South Africa is less likely than any other country in the

Global Entrepreneurship Monitored (GEM) sample to have a new SME survive in the early phases of its existence, as evidenced by the 2015/2016 Global Report. However, a high proportion of SMEs failing in South Africa is a major problem.

A survey done by Lautenbach, Johnston, & Adeniran-Ogundipe (2017), states that in terms of entrepreneurship activity in its early stages, South Africa lags behind its competitors. Leveraging small businesses' ability to create jobs and fostering small business growth are two strategies for solving unemployment (Mutalemwa, 2015). According to a study done by Evans, Josephine, & Yeboah (2015), South Africa has the greatest failure rate in the world with 75% of SMEs failing to grow into successful enterprises. Due to an unfavorable economic environment characterized by adversarial regulatory requirements, high taxes, inflation, and volatile and unpredictable exchange rates, SMEs find it challenging to operate and must struggle to turn a profit to exist (Olawale & Garwe, 2010). Below is a discussion of the main issues that African SMEs must deal with. The most pressing challenges are:

- **Access to financing:** According to Muriithi (2017), a sufficient supply of financial resources is necessary for the expansion of SMEs. Lack of funding has been identified as a constraint to this growth. In actuality, it is a widely acknowledged issue that SMEs face that they cannot acquire loans or financing.
- **Poor management:** According to Fouad (2013), poor management is a significant issue that businesses throughout the world must deal with. This results from the lack of managerial expertise that the majority of SME operators or managers exhibit. Many business owners lack the necessary education and expertise to run their companies, so they tend to manage by trial and error and are more focused on short-term benefits than long-term strategy.
- **Competence and capability:** The absence of managerial competency is a significant problem for many SMEs. This refers to the knowledge, abilities, and expertise of business owners and managers. To develop skills, which in turn lead to competencies, a manager must be able to mix both tangible and intangible resources (Murithi, 2017).
- **Government support:** According to Kamunge, Njeru, & Tirimba (2014), in every country, the government continues to play a crucial role in assisting and supporting SMEs. The government is the one who establishes the favourable or unfavourable business environment.

When the government gives the SME sector minimal attention, it is likely to suffer, which makes it difficult for many enterprises to exist. In addition to harming the sector, a government that does not assist SMEs sees a downturn in its economic growth. The environment that the government has built for SMEs in terms of pay structure, taxation, licensing, possibilities, technological support, and infrastructure determines whether they will succeed or fail.

- **Technological development:** According to Das, Kundu, & Bhattacharya (2020), one of the key elements affecting a company's ability to compete in both domestic and foreign markets is technological progress. The majority of SMEs struggle to adapt to the rapid technological advancements that are needed to better fulfill market needs. Herrington, Kew, & Mwanga (2017), claim that 71% of families in the rest of South Africa do not have access to the internet, which severely restricts the production and efficiency of businesses.

2.3 Information conceptualization

Understanding the term 'information' more is required to comprehend how the information relates to information security and SMEs. To grasp the terminology, the meanings of information and its role as well as relevance in organizations are discussed below.

2.3.1 Defining information

One of the most valuable resources for organizations is information (Redman, 2008). "Information is now frequently exchanged, bought, traded, found, generated, and applied to work in the same manner that goods and services are" (Davenport & Prusak, 1998). Even though it is frequently developed to facilitate the efficient manufacture and distribution of the primary market offering of the organization, information can also be sold to customers as a stand-alone product (Orna, 2004). Due to its significance for the effective running and strategic development of their operations, organizations are becoming more and more concerned with protecting their information (Bunker, 2012).

Information is created from extracted and reformatted raw data (Winne, Nesbit, & Popowich, 2017). According to Loia, D'Aniello, Gaeta, & Orciuoli (2016), "Verified and accurate raw data that is presented within a context that gives it meaning and importance leads to better comprehension and less uncertainty and is provided within a context that gives it a purpose and meaning". Thus, information and data that has been examined and presented in a way that is useful to both companies and individuals.

Information definitions are significantly more consistent and straightforward than raw data definitions (Sawicki, Wegener, Clark, & Fabriga, 2013). Three authors define information as: "*Organized data*" (Saint-Onge, 2002); "*data provided with relevance and purpose*" (Drucker, 2001); "*interpreted data*" (Gibbert, Leibold, & Probst, 2002). It is clear from these definitions that humans are crucial to arranging raw data in a meaningful way.

2.3.2 The importance of information

Increasingly, organizations understand the importance of information in gaining a competitive advantage and sustaining success (Xiang, Magnini, & Fesenmaier, 2015). For a company to succeed, managers would agree that good information is essential. Adaptability and responsiveness to the environment are essential for a company to survive and thrive (Harraf, Wanasika, Tate, & Talbott, 2015). Companies with more knowledge are thought to be able to make better decisions, become more efficient, and have a competitive advantage over their competitors (Efrat, Hughes, Nemkova, & Souchon, 2018).

According to Halawani & Rahman (2013), small and medium-sized businesses require a large amount of information for their managers, and their environment is extremely information rich. The information that every business relies on is a precious asset that must be protected (Bruening, Sotto, Abrams, & Cate, 2008). Business and stakeholder goals can be satisfied by extracting value from data and information. To meet social, environmental, and sustainability goals, information must be managed correctly (Oláh, Kitukutha, Haddad, & Pakurár, 2018). The employees of businesses often have access to sensitive information, including social security numbers, tax numbers, credit card numbers, or health records (Salahdine & Kaabouch, 2019). "Employee processing and use of information are crucial in preventing errors, abuse, or erroneous disclosure, which could result from ignorance, fraud, or wilful damage" (Xiang, Magnini, & Fesenmaier, 2015).

Information is becoming more valuable, making it easier for hackers, spammers, criminals, and terrorists to access and abuse it (Wall, 2007). Moreover, recent innovations in IT infrastructures, such as the Internet and cloud computing, have compelled organizations to increase their attention to information security (Morin, Aubert, & Gateau, 2012). As a result, security incidents and attacks are still on the rise (Symantec, 2015), although not all security incidents and breaches are caused solely by technology vulnerabilities and shortcomings (Symantec, 2015). Indeed, it is "frequently claimed that the human component of any organization's information security defences is the weakest link"

(Bulgurcu, Cavusoglu, & Benbasat, 2010). Virus infections, disruptive software, staff misuse of information systems, and breaches of confidentiality were documented along with technical issues (Doherty & Tajuddin, 2018). To explore all the issues related to information security, the study will provide an overview and an in-depth discussion below.

2.4 Overview of Information security (InfoSec)

The year 2015 was marked by major hacks and data breaches that made information security global news (Laybats & Tredinnick, 2016). Information security should be considered an important security tool for not just individuals but organizations and businesses as well. "Information security is of great importance and interest to everybody in the world of technology today, whether you are a mobile phone or a personal computer user, this is why information security is of the most important in our everyday life, and in the IT technology fields" (Alhassan & Adjei-Quaye, 2017) The concept of information security encompasses more than just IT security; it also involves legal compliance, governance, and workflow issues (Brown, Gommers, & Serrano, 2015). Therefore, organizations view information security as an integral part of the planning and execution of their business activities, rather than as a separate issue (Mukherjee & Paul, 2013). According to AlKalbani, Deng, & Kam (2015), as organizations become more reliant on information systems, they face new challenges to safeguard their critical information from different security threats, which have direct consequences on their liabilities, credibility, and monetary loss. The following section is a more in-depth explanation and definition of information security, along with all its aspects.

2.4.1 Defining Information security (InfoSec)

As the name implies, information security or InfoSec is the process of protecting information from "unauthorized access, use, disclosure, disruption, modification, inspection, recording, or destruction". (Alhassan & Adjei-Quaye, 2017). In general, it refers to data and information regardless of its form (e.g., electronic or physical). Other authors describe information security as "the domain that deals with the confidentiality, integrity, and availability of the information" (Tchernykh, Schwiegelsohn, Talbi, & Babenko, 2019). Moreover, this definition directly relates to the CIA triad of information security. In addition, a critically important aspect of information security is to ensure the confidentiality, integrity, and availability of information and related assets within an organization, which prevents operational loss (Goldstein, Chernobai, & Benaroch, 2011).

From the perspective of Information security, it is seen as a holistic approach that supports internal collaborators, business partners, vendors, customers, and other stakeholders in addition to the assets that make up the organization's corporate systems (Correia, Gonçalves, & Teodoro, 2017). More authors describe and define information security from their perspective. Authors Kirsch & Boss (2007), points out that information security compliance enforcement is becoming more and more of a priority. Also, according to AlKalbani, Deng, & Kam (2014), information security is also defined as the successful use of information security standards and procedures to safeguard data in public organizations. From a management perspective, the authors Kolkowska & Dhillon (2013) define information security as including both technical and non-technical information handling operations. Therefore, numerous technological, operational, and managerial controls are included in the management of information security (shown in Figure 1 below) to protect data and prevent the improper use of information systems (Baker & Wallace, 2007).

To put more focus on information security threats, it can be categorized into a variety of distinct categories (Laybats & Tredinnick, 2016):

- Information security threats can be seen as the purposeful results of deliberate actions, including deliberate data theft, leaks, or breaches, malicious software, spyware, denial-of-service assaults, and industrial espionage.
- Information security threats can be seen as the unintended repercussions of intentional behavior, such as data leaks, thoughtless disclosure of information, reckless deletion of information, unintentional breach of confidentiality, etc.
- Information security threats can be seen as the unintended results of unintentional actions, such as data loss or data destruction due to an accident.

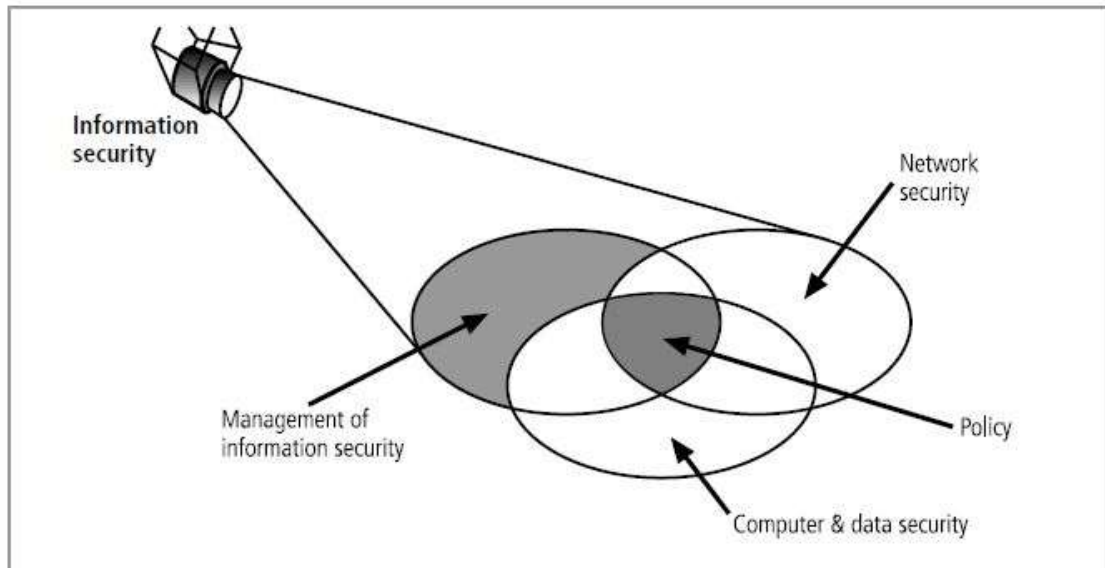


Figure 1: Components of Information security (Source: Whitman & Mattord, 2011)

2.4.2 Information security principles

In information security, data and information systems are protected from “unauthorized access, use, disclosure, disruption, alteration, or destruction” (Haris, Sarijan, & Hussin, 2017). “A key principle of information security is that of ensuring the confidentiality, integrity, and availability of information of authorized use by approved users” (Gladden, 2017). Together the terms are called the CIA triad. The CIA triad was created in the 1990s as a generally accepted method of expressing security needs for information assets (Shoufan & Damiani, 2017). Later, it was frequently expanded to include more security features or to deal with certain domains (Frühwirth, 2009). It protects data availability by ensuring that data is always accessible, ensures confidentiality by preventing unwanted access, and promotes integrity and authenticity by ensuring that data is complete and correct (Alhassan & Adjei-Quaye, 2017). Information processed by an organization must be secured to guarantee that its confidentiality and integrity are maintained and that it is easily accessible when needed to reduce the risk of financial loss (Da Veiga & Martins, 2015).

There is frequent use of the phrases "confidentiality," "integrity," and "availability" in the field of information security, both in academic research and in practice (Aminzade, 2018). Figure 2 below depicts the CIA triad as the information security principles, According to the authors Samonas & Coss (2014), the CIA triad is the main component of information system security controls. In addition, the authors assert that these three fundamental terms have impacted both theoretical and practical

understandings of information security. In these security practices, technical controls are used to protect information's confidentiality, integrity, and availability (Andress, 2014). A study done by Merkow & Breithaupt (2014), defines the CIA triad as a fundamental concept in information security to ensure the protection of the three sections of the triad as a key step in creating any secure system. However, to the National Institute of Standards and Technology (NIST), “the CIA triad is used as a rating system with five levels (A to E) for each service rated based on three dimensions of security: Confidentiality, Integrity, and Availability” (Shoufan & Damiani, 2017). Countries like the USA, which use the CIA triad as a standard practice, use the rating system more commonly. The three concepts of the triad are discussed in more detail in the next sections.



Figure 2: The information security triad (Source: Nikander, Manninen, & Laajalahti, 2020)

2.4.2.1 Confidentiality

The first concept in the CIA triad is described as confidentiality. According to Lundgren & Möller (2014), the term confidentiality in the triad refers to “property that information is not made available or disclosed to unauthorized individuals, entities, or processes”. To maintain confidentiality, systems must help to protect data, as well as ensure that only trusted individuals have access to it (Shoufan & Damiani, 2017). Another definition of confidentiality according to authors Samonas & Coss (2014), is the concept confidentiality is rooted in the military mindset regarding top-down authority and control over those with access to information on a need-to-know basis. Therefore, keeping data, information, and knowledge security is key to the success of any organization (de Oliveira

Albuquerque, García Villalba, Orozco, Buiati, & Kim, 2014). A practical example of practicing confidentiality using an ATM is to require users to practice a two-factor authentication which involves both an ATM card and a pin code before they are allowed to access data (Fruhlinger, 2020).

2.4.2.2 Integrity

As part of the CIA triad, integrity is considered the second concept. (Lundgren & Möller, 2014), defines the integrity concept as a “property of accuracy and completeness”. It should be highlighted that when this type of violation occurs, the intruder may not always be aware of the information that has been altered. (Samonas & Coss, 2014). According to de Oliveira Albuquerque, García Villalba, Orozco, Buiati, & Kim (2014), integrity in information security refers to the inability of data to be altered without permission. The authors further assert that professionals in information security are entrusted with figuring out how to put measures in place to prevent integrity breaches. Other experts have found ways to improve information security through deterrence measures (Qadir & Quadri, 2016). A practical example of practicing integrity through the use of ATMs and bank software is by ensuring that all cash withdrawals and any transfers done will reflect in the user’s bank account (Fruhlinger, 2020).

2.4.2.3 Availability

The third concept in the CIA triad is known as availability. Availability is described as the “property of being accessible and usable upon demand by an authorized entity” (Lundgren & Möller, 2014). This is an indication that information must be accessible when needed for information systems to fulfill their purpose (de Oliveira, Villalba, Orozco, Buiati, & Kim, 2014). The authors further assert that all information systems, networks, databases, information assets, storage devices, etc. must be reachable by those with permission to handle them to acquire such property. A practical example of practicing availability is that ATMs are available in public places for users and are accessible when the banks are closed (Fruhlinger, 2020).

2.4.3 Information security policies (ISP)

According to Sommestad, Hallberg, Lundholm, & Bengtsson (2014), an information security policy includes all the intentions, principles, rules, and guidelines that are set by management for employees to abide by. The authors further state that the information security policy aims to provide guidance and assistance to management for information security (ISO/IEC, 2009). It should outline information security responsibilities, permissible computer resource usage, the penalties for violating security

policies, and the training that various sorts of personnel should get (Chipperfield & Furnell, 2010). The main principle is to improve the organization's level of information security by compliance with an effective information security policy (Ifinedo, 2012). It is, however, far from simple for organizations to achieve compliance with information security policies.

According to Chen & Li (2014), “management uses an information security policy to distinguish between employee behaviours that are either permitted or banned, as well as the associated penalties if the forbidden behaviours occur”. The goal of an information security policy, on the other hand, is to give management guidance and support per business requirements and regulations when it comes to information security (Diamantopoulou, Tsohou, & Karyda, 2019). There are obstacles to the effective implementation of information security policy in the management policy, dissemination, user awareness, and user behaviour areas (Alotaibi, Furnell, & Clarke, 2016). It is evident that an organization's well-being when protecting its information benefits greatly from an information security policy (Sommestad, Hallberg, Lundholm, & Bengtsson, 2014). However, putting into practice an efficient information security policy is considered challenging.

2.4.4 Information security standards

In general, standards are a set of requirements for products or systems, whether they are accountability standards, technical standards, or information security standards (Tofan, 2011). In terms of information security, there are currently a few primary standards in place on a global level. The first standard is the ISO/IEC 27002:2013 which is a series of information security standards (Meriah & Rabai, 2019). Because it is backed by the internationally prestigious names of the International Electrotechnical Commission and the International Organization for Standardization, it is the most recognizable standard (Tofan, 2011). “ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation, and management of controls taking into consideration the organization's information security risk environments” (ISO/IEC 27002:2013, 2013).

Another standard to consider is the NIST SP800 group of standards has been published by the National Institute of Standards and Technology (NIST) in the United States (Piggin, 2013). According to Ajijola, Zavarsky, & Ruhl (2014), the NIST is a non-regulatory agency within the US commerce department. Further, the authors state that NIST develops and applies technology, measurements, and standards to the technology industry. In addition, “security and privacy are among the main concerns of the SP 800 publications, which are designed to meet the information and information system

security and privacy needs of the US Federal Government” (NIST Special Publication 800-series General Information, 2018).

By adopting standards, personal security systems can be compared with a given international benchmark that is accepted worldwide (Tofan, 2011). The purpose of standards is to ensure that products and services meet desirable characteristics, such as safety, reliability, efficiency, and interchangeability, at a reasonable price (Aswal, 2020). For an organization to meet its requirements, information security standards are required (D'Arcy, Herath, & Shoss, 2014). In addition, establishing controls over business relationships with other organizations is also important. To meet business needs, organizations can greatly benefit from shared best practices at an international level by implementing one of these standards (Tofan, 2011).

2.4.5 Information security controls

To apply security controls, the information system should be assessed for risk (Bhaskar & Ahson, 2008). According to Almeida & Respício (2018), these controls must be implemented in a manner that ensures an adequate level of protection. However, the authors assert that security investments must be compatible with the economic constraints of the organization, as well as the vulnerabilities and threats that exist in the organization. Another definition of information security controls is “the safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information” (Abazi, 2018).

Security controls can be categorized into three different categories as shown in Figure 3 below. Information security control is either administrative, technical (also known as logical), or physical (Yau, 2014). In the section that follows, each security control is briefly described.

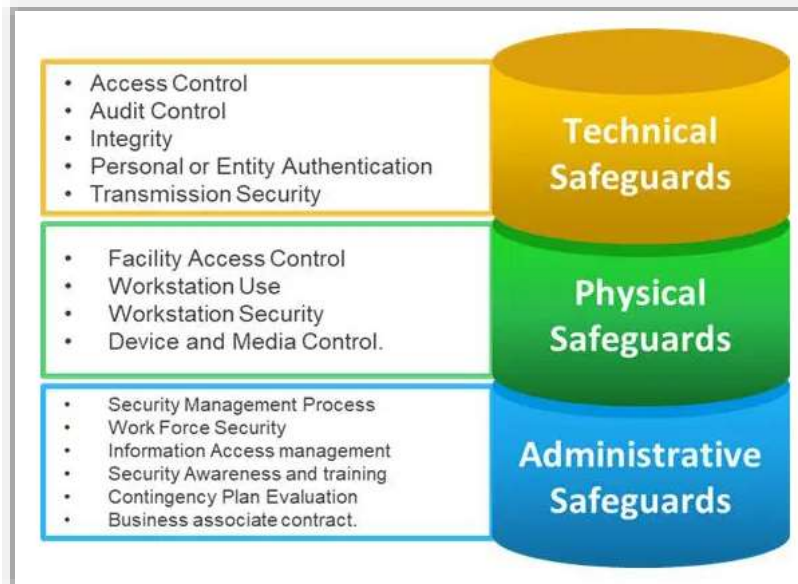


Figure 3: Security controls (Source: Cyber Security Framework, 2018)

2.4.5.1 Administrative controls

An organization can govern employee behaviour by using administrative controls, also referred to as management controls (Arjaliès & Mundy, 2013). According to Yau (2014), administrative security controls, sometimes referred to as procedural controls, are policies and guidelines implemented to specify and direct staff behaviour when managing sensitive information on behalf of the firm. The author also indicated that such controls educate the public on how the company should be managed and how daily operations should be carried out. Sattarova Feruza & Kim (2007), mentions that in addition to being a form of administrative control, laws and regulations made by governmental entities also provide businesses with information. In addition, Yaokumah (2017) describes administrative security controls as being in the form of a policy that can be implemented by using aspects of physical and technical controls. For instance, a network access control program may use a technical control to check for antivirus software when a computer tries to connect to the network despite a security policy that prohibits computers without it from doing so (Wang, Wei, & Vangury, 2014).

2.4.5.2 Physical controls

To reduce security risks in organizations, a variety of security measures are being explored. Physical security controls are one of those measures. DiMase, Collier, Heffner, & Linkov (2015), refers to physical security controls as tools to employ to maintain physical security that includes people, systems, and other techniques. Physical controls can be considered the first line of defence for an

organization. These measures prevent unauthorized people from entering facilities (Rainer & Cegielski, 2010). As a result, access to and from organizational contexts is controlled by these restrictions. These measures are the simplest and most affordable to apply, but they are frequently the most successful (Ndolo, Ogara, & Liyala, 2018). A few examples of common physical controls are walls, doors, fences, gates, locks, badges, guards, bollards, cameras, and alarm systems. To manage the physical environment in companies, such as physical intrusion detection systems and physical protection systems, physical controls also refer to those methods (Andress, 2011).

2.4.5.3 Technical controls

Technology plays an important role in reducing security risks in organizations. Technical security controls are one way to reduce risk. According to Bhaskar & Ahson (2008), technical security controls, also known as logical controls, refer to limiting access to a system. Another author states the idea that logical security components are made up of hardware and software features that help to protect the security and integrity of data, programs, and operating systems (Schweitzer, 1990). Any system user who may sign on or each application that may be called on by the computer to process files with predetermined value factors can be identified, authenticated, authorized, or limited to just doing specific previously specified actions by an effective logical security system (Ndolo, Ogara, & Liyala, 2018). These consist of file permissions, firewalls, access control lists, and antivirus software.

2.4.6 Information security compliance

In an emerging information systems era, organizations need to have information security compliance in place to ensure that the organization's data and information are protected. According to Lee, Lee, & Kim (2016), information security compliance refers to implementing information security policies and standards to safeguard and secure the organization's data. Another author describes information security compliance as the procedure for monitoring and evaluating the organization's systems through the implementation of information security standards and policies (AlKalbani, Deng, & Kam, 2014). "The adoption of information security compliance ensures that information security mechanisms can work together effectively to protect the critical information in organizations" (Ifinedo, 2014). It complies with security criteria, enhancing stakeholder confidence and trust in the organization. As a result, the effective approach to information security compliance assures the successful adoption of information security in organizations (Herath & Rao, 2009).

Several studies have been done based on information security compliance in organizations. For example, AlKalbani, Deng, Kam, & Zhang (2017) investigated the impact of institutional pressures on information security compliance in organizations. Kim & Kim (2017), examined how information security compliance behaviour is affected by compliance knowledge and support systems. Sommestad, Hallberg, Lundholm, & Bengtsson (2014), reviewed quantitative research that examined factors influencing compliance with information security policy. Safa, Von Solms, & Furnell (2016), examined the information security policy compliance model in organizations. These studies have focused primarily on information security compliance in organizations and not primarily on small-medium enterprises.

2.5 Information security governance

An organization's survival needs to take a proactive approach to security. As part of executive management's responsibilities, security governance ensures that goals are met, risks are appropriately managed and the enterprise's resources are used responsibly (Fay & Patterson, 2018). A brief overview of the King IV report, the Electronic Communications and Transactions Act (ECT), and the Protection of Personal Information Act (POPI) is provided in this section of the study.

2.5.1 King IV

The concept of good corporate governance is principally about effective, ethical leadership (Naidoo, 2012). The King IV report was released in November 2016, elevating South Africa to the position of one of the world leaders in corporate governance (Ernst & Young, 2016). The KING IV report provides a seven-part holistic approach (see Figure 4) to governance for public and private sector organizations nationwide (Ferguson, 2019). “Principles one and two of King IV Report on Corporate Governance which came into effect on 1 April 2017 indicates that governing body should lead ethically and effectively, while principle two demonstrates that the governing board should guide the ethics of organizations in a way that supports the establishment of ethical culture” (Chauke, 2019). More details on the King IV report will follow in the next sections of the chapter.



Figure 4: King IV principles (Source: Ferguson, 2019)

2.5.1.1 Outcomes of King IV code

According to the King IV Code, the following principles outcomes interact (PwC, 2016):

- **Ethical culture outcomes:** Leading ethically and effectively is the responsibility of the governing body. Ethics should be managed effectively by the organization's governing body. Organizations should ensure that they are responsible corporate citizens through their governing bodies.
- **Performance and value creation outcomes:** The process of creating value includes strategy, risk and opportunity, performance, and economic development. For stakeholders to be able to make accurate and sustainable assessments of the organization's performance, reports and other disclosures should be provided by the governing body.
- **Adequate and effective control outcomes:** As the organization's custodian of corporate governance, the governing body should act as the organization's focal point. To discharge its duties and responsibilities, the governing body should have a balanced composition of skills, experience, adequate and effective control, diversity, independence, and knowledge.

- **Governance functional areas outcomes:** Risk and opportunity should be managed by the governing body in a way that helps the company define its core purpose and establish and meet its strategic goals. Information and technology should be regulated by the governing body in a way that aids in the company's development and achievement of its strategic goals as well as the definition of its primary purpose.
- **Trust, good reputation, and legitimacy outcomes:** The governing body should make sure that a stakeholder-inclusive approach is used when making decisions that are in the best interests of the organization. This approach should take into account and balance the legitimate and reasonable needs, interests, and expectations of all stakeholders.

2.5.2 Electronic Communications and Transactions Act (ECT)

An effective piece of legislation that aims to place South African law on the radar of the rapidly changing international community is the Electronic Communications and Transaction Act 25 of 2002 (Mabeka, 2021). All electronic communications and transactions in South Africa are governed by the ECT Act (Maritz & Hattingh, 2015).

2.5.2.1 Electronic signatures defined

The Electronic Communications and Transactions Act 25 of 2002 (the "ECT Act") has been in force for more than ten years. Section 1 of the Bill makes a significant modification to e-commerce by proposing a new definition of the term "electronic signature" (Eiselen, 2014). The most current definition is as follows:

“Electronic signature means data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature” (Electronic Communications and Transactions Act 25, 2002)

The following is the proposed revised definition of an electronic signature:

“Electronic signature means a sound, symbol, or process that is (i) uniquely linked to the signatory; (ii) capable of identifying the signatory; (iii) created using means that the signatory maintains and which are under his control; (iv) linked to the data to which it relates in such a manner that any

subsequent change of the data can be detected; and (v) intended by the user to serve as a signature”
(Electronic Communications and Transactions Amendment Bill, 2012)

2.5.2.2 Purpose of act

The ECT Act's purpose states that the Act's objective is to (Coetzee, 2004):

- To make provisions for the regulation and facilitation of electronic transactions and communications.
- To make provisions for the Republic's national e-strategy development.
- To encourage SMME use of electronic transactions and universal access to electronic communications and transactions.
- To support the development of human resources for electronic transactions.
- To avoid information system abuse.
- To promote the usage of services provided by e-government.
- To make provisions for matters related thereto.

2.5.3 Protection of Personal Information (POPI) Act

Due to the rise of the information age and the enormous increase in the value of personal information, "identity theft" is the most common crime of the new millennium that has emerged (Dala & Venter, 2016). According to Titus (2011), "legislation relating to the protection of personal information consequently aims to safeguard people from identity theft and provides extensive institutional benefits like the protection of an institution's brand, image, and reputation, enhancing credibility as well as promoting consumer confidence and goodwill". From a South African perspective, legislation in this area took the form of the Protection of Personal Information (POPI) Bill which was first published for comment in 2005 (Stein, 2012).

South Africa received its data protection legislation - the Protection of Personal Information (POPI) Act - in November 2013 and is expecting the government to appoint an Information Regulator to enforce the letter of the law (De Bruyn, 2014). The act protects the privacy rights determined by section 14 of the South African Constitution which specifies that "everyone has the right to privacy" (Constitution of the Republic of South Africa No 108, 1996). According to the Republic of South Africa (2013), the 12 chapters of the POPI Act, which comprise 8 requirements for the lawful handling of personal data, encourage the protection of personal information by the South African public and commercial organizations.

The following section will briefly describe the information regulator of the POPI act, the computer ethics, the violations of the POPI Act, the principles of the act as well as the challenges for SMEs.

2.5.3.1 Information Regulator

The Information Regulator is a government body that is in charge of enforcing the POPI Act (Sekgweleo & Mariri, 2019). It was established under Section 39 of the POPI Act 4 of 2013 and reports to the national assembly (Protection of Personal Information Act 4, 2013). It has the authority to enforce the Promotion of Access to Information Act of 2000 and the Protection of Personal Information Act of 2013 (Information Regulator, 2017).

The head of the Information Regulator, Advocate Pansy Tlakula, is one of five members chosen by South Africa's president in 2016 (The Department of Justice and Constitutional Development, 2020). Although there has been some delay, The Information Regulator is actively filling positions at its office (Bratt, 2018). Regarding whether or not to schedule three entities under the Public Finance Management Act, they and Treasury are at odds (Republic of South Africa, 2013). According to the regulatory structure of the regulator, the chief executive will serve as the accounting officer (Calland & Tilley, 2018). Instead, Treasury opted to assert that the Public Finance Management Act requires Pansy Tlakula, the chair of the regulator's board of directors, to serve as the accounting officer (Sekgweleo & Mariri, 2019).

2.5.3.2 Violation of the POPI Act

It is a crime to violate the POPI Act in South Africa (Sekgweleo & Mariri, 2019). If their personal information has been compromised, individuals may be able to launch civil actions in specific circumstances under the statute (Swartz & Da Veiga, 2016). For violations of the act, the Information Regulator may "impose a fine of up to R 10 million, a term of imprisonment of up to 10 years, or a combination of a fine and jail sentence under Chapter 11 of the POPI Act" which includes offenses, penalties, and administrative fines (De Bruyn, 2014). In addition to the enforcement proceedings and the financial consequences outlined above, the reputational damage can also have a substantial impact on businesses if the data protection authority publishes a finding of non-compliance with the privacy legislation (Tubbs, 2020).

The regulator has the right to take legal action in any of four categories when an organization violates the POPI Act (Botha, Eloff, & Swart, 2015):

- Up to R10 million in fines could be imposed on an organization. Depending on several variables, the fine amount may change.
- An organization could receive a prison term of up to ten years.
- An organization may be ordered to stop processing personal data by the regulator. This might lead to a business closing.
- The regulator could file a civil lawsuit on behalf of another organization.

2.5.3.3 The POPI Act principles

When studied, it becomes clear that certain safeguards must be implemented to comply with the prerequisites or principles indicated in Table 3. According to surveys done by Botha, Eloff, & Swart (2015), corporations in South Africa have historically had limited accountability and are sluggish to adapt to the present climate, therefore it is clear that SME businesses face several serious issues.

Table 3: The eight principles of the POPI Act (Source: POPI Act 4, 2013)

Principle	Description
1. Accountability	The responsible party, who is the individual or organization handling the information, is required to make sure that all eight guidelines are followed.
2. Processing Limitation	The amount of information that can be processed should be limited, indicating that it should only be done legitimately and sparingly.
3. Purpose Specification	A clear, legitimate reason for collecting personal data must exist. The goal should be connected to the responsible party's action, and the responsible party must make sure that the goal is communicated to the data subject.
4. Further Processing Limitation	Any additional processing of the data must be consistent with the initial intent behind its collection.
5. Information Quality	The data must be true, accurate, and not deceptive. If necessary, the data can be updated while keeping in mind the reason it was originally gathered.

6. Openness	There should be transparency, which calls for alerting the information regulator before any information processing takes place. The data subject should be informed that their information was obtained, and the processing should be recorded in a register.
7. Security Safeguards	It is important to preserve the accuracy of any personal data that has been gathered.
8. Data Subject Participation	The data subject is entitled to free access to any information that the responsible party may retain upon request.

2.5.3.4 Challenges for SA SMEs

For SMEs, marketing is a top priority, and they regularly promote questionable methods (Botha, Eloff, & Swart, 2015). Small businesses have been known to use any form of electronic communication, including direct marketing and advertising, to carry out their marketing strategy to attract the consumer's attention (De Bruyn, 2014). Once the new privacy legislation takes effect, this form of marketing will need to take a different direction. According to POPI Act, marketing is only permitted with the data subject's permission. As a result, SMEs will need to re-evaluate their strategy for reaching out to potential clients using electronic media (Protection of Personal Information Act 4, 2013).

According to the Protection of Personal Information Act 4 (2013), which focuses on direct marketing, which is mostly conducted through electronic communication channels, enterprises must adhere to the following standards:

- Before engaging in any electronic marketing, the customer's consent must be secured.
- The choice to consent to receive marketing information about the service or product provided (as well as similar services and products) must be offered when collecting personal information from new clients.
- Existing customers must be given the option to "opt-out" of receiving marketing communications at any time if their personal information has already been collected.
- For each marketing communication technique, the name of the supplier and contact information the consumer might use to "opt-out" must be published.

2.6 Information security theories and frameworks

Following are some theories and frameworks that fit well with the components of information security compliance. The institutional theory focuses on how the rules and guidelines of an organization and management practices influence social behaviour. The Technological-Organizational-Environmental framework is a theoretical framework that explains technology adoption in organizations.

2.6.1 Institutional theory

Many businesses use the institutional theory to better understand how institutional pressures affect information security compliance (DiMaggio & Powell, 1983). According to this theory, companies must meet external expectations to gain the legitimacy of their stakeholders (Appari, Johnson, & Anthony, 2009). The institutional theory's core principle is that organizational practices and behaviours are influenced by the social and cultural factors in their environmental settings (Luna-Reyes & Gil-Garcia, 2011). These influences could, for instance, influence how an organization is created, run, understood, and assessed in a certain circumstance. Organizations employ the institutional theory to demonstrate that the organizational compliance procedure is significantly impacted by current laws, regulations, and public opinion (Liang, Saraf, Hu, & Xue, 2007). This is so that the institutional theory may be utilized to more clearly describe how the organizational environment can affect the creation of a formal information security strategy in organizations (AlKalbani, Deng, Kam, & Zhang, 2017).

To comprehend how institutional influences affect an organization's information security compliance, a model created by DiMaggio & Powell (1983) is commonly employed (Singh & Alshammari, 2020). According to this concept, companies must adhere to external expectations to be taken seriously by stakeholders (Appari, Johnson, & Anthony, 2009). Previous studies have reported that this legitimacy can be preserved by strategically reacting to outside influences (Cavusoglu, Son, & Benbasat, 2015). However, DiMaggio & Powell (1983) claimed that organizations gradually settle on a common set of procedures and behaviours. They identified three factors and analyzed how they affect the isomorphic acceptance of adopted behaviours and practices throughout the entire organizational field. Coercive (restraining), normative (learning), and mimetic (cloning) forces (Cavusoglu, Son, & Benbasat, 2015). The following section goes into further information about these three forces.

2.6.1.1 Coercive pressures

Coercive pressures are characterized as formal and informal forces used for social actors to embrace the same views, behaviours, and practices when they perceive pressure from more powerful actors to do so (DiMaggio & Powell, 1983). The prior empirical evidence indicates that coercive pressures may originate from a range of sources at the organizational level, including regulatory authorities, suppliers, customers, parent firms, and other important stakeholders (Teo, Wei, & Benbasa, 2003). There are two main categories of coercive pressures: regulation and competition. Harcourt, Lam, & Harcourt (2005), claims that there may be increased regulatory pressure from governmental and corporate regulatory bodies. The second category includes threats of losing a competitive advantage which leads to competitive pressures. Previous studies have reported how coercive isomorphism pressures affect the acceptability of innovations. For instance, authors Zhu, Kraemer, & Dedrick (2004), suggested that the regulatory framework is crucial to the spread of e-business. Also, Wang & Cheung (2004), discovered that coercive coercion was favourably connected to the adoption of e-business by travel companies.

2.6.1.2 Normative pressures

The professionalization of areas and disciplines creates normative pressures when social actors unintentionally but freely adopt the same attitudes, behaviours, and practices as other actors (Jan, Lu, & Chou, 2012). The community's expectation that organizations must uphold to act as responsible citizens in a particular situation is the source of normative pressures (Appari, Johnson, & Anthony, 2009). According to institutional theory, social actors are more likely to duplicate a particular action if it has already been taken by a significant number of other players (Shi, Shambare, & Wang, 2008). The assumption of legitimacy, not necessarily appropriateness, leads social actors to be forced to adopt particular behaviours (Flanagin, 2000). However, no powerful individuals or organizations are forcing this copying or imitation, and it is not intentional (Shi, Shambare, & Wang, 2008).

2.6.1.3 Mimetic pressures

Mimetic pressures encourage social actors to actively seek out examples of acceptable behaviours and practices to imitate by deliberately and consciously adopting the identical behaviours and practices of other high-status and successful actors in the delusion that successful actors' activities are more likely to have favourable effects (DiMaggio & Powell, 1983). Additionally, actors can replicate through imitation with little investment in search and experimentation expenses and without taking the risks associated with being the first to do something (Teo, Wei, & Benbasa, 2003). The act of

duplicating or imitating another person's behaviour is known as mimetic isomorphism. As a result of these behaviours, firms replicate the successful behaviours and practices of other, similarly situated organizations in their surroundings (Safa, Von Solms, & Furnell, 2016). Organizations that publicize their perceived benefits put pressure on other organizations to follow suit with their activities and behaviours (AlKalbani, Deng, Kam, & Zhang, 2017).

2.6.1.4 The effectiveness of Institutional theory

The literature available provides excellent examples of how the institutional theory may be used to understand how particular technological advancements are adopted (Cavusoglu, Son, & Benbasat, 2015). For instance, Butler (2011) uses the institutional theory to demonstrate that sustaining existing ties and a high level of established commitments are the two institutional elements that influence the growth of web-based systems in organizations. According to Cavalluzzo & Ittner (2004), “the implementation of management control systems that raise operational productivity in public organizations is influenced by the acceptance of legislative requirements”. Using the institutional theory, Liang, Saraf, Hu, & Xue, (2007) demonstrated how existing laws and regulations as well as public sentiment have a substantial impact on organizational behaviour. Zheng, Chen, Huang, & Zhang (2013), created and tested a theoretical framework to examine how public administration organizations are implementing government-to-government (G2G) information technologies. These studies show that institutional theory offers a solid theoretical foundation for comprehending the adoption of technological breakthroughs in organizations from an institutional perspective.

2.6.2 The National Cybersecurity Policy Framework (NCPF)

The Minister of State Security in South Africa reacted to the National Cybersecurity Policy Framework for the first time in 2015. For all governments, creating, implementing, and reviewing national cybersecurity policies has become a top priority (Sabillon, Cavaller, & Cano, 2016). According to van Vuuren, Leenen, Phahlamohlaka, & Zaaïman (2013), with this framework in place, the national governments must provide for, oversee, and protect their citizens' national security, which involves cybersecurity. “The urgent need to address national cybersecurity protection is driven by the growing cybersecurity challenges and threats as well as dependence on technology around the globe” (Jang-Jaccard & Nepal, 2014). Consequently, any cybersecurity policy should have measures and guidelines to support and maintain cybersecurity.

2.6.2.1 Purpose of the NCPF

The NCPF places a strong focus on cross-government coordination in its implementation (Bote, 2019). The implementation of the policy framework is credited to clusters including justice, crime prevention, and security (Braga, Welsh, & Schnell, 2015). As stated by the NCPF report, the Cybersecurity Response Committee (CRC) is presided over by the Director General of State Security, who also communicates with the leaders of other relevant ministries and agencies (Bote, 2019). The CRC's responsibilities include making decisions, strategizing, and prioritizing areas for threat identification, intervention, and evaluation. Therefore, this NCPF conveys as per the National Cybersecurity Policy Framework, (2015):

- “Measures to address national security in terms of cyberspace”;
- “Measures to combat cyber warfare, cybercrime, and other cyber ills”;
- “The development, review and updating of existing substantive and procedural laws to ensure alignment”; and
- “Measures to build confidence and trust in the secure use of ICT”.

2.6.3 Technological-Organizational-Environmental framework (TOE)

Tornatzky and Fleischer created the Technological-Organizational-Environmental framework in 1990 as "the process of technological innovation" (Baker, 2012). The TOE framework was created to explain the organizational factors that influence an organization's decision to adopt cutting-edge technology (Ahmi, Saidin, & Abdullah, 2014). Comparing the TOE framework to other adoption models for evaluating technology adoption, use, and value generation, the incorporation of technological, organizational, and environmental aspects has proven useful (Gangwar, Date, & Ramaswamy, 2015). Additionally, the TOE framework is not constrained by limits on industry or business size (Wen & Chen, 2010). Furthermore, the TOE paradigm has been thoroughly examined in IT/IS adoption studies and has consistently reported empirical evidence (Oliveira, Thomas, & Espadanal, 2014).

The framework established three crucial concepts that should be taken into account while implementing security. The first component is called "technological factors in security," and it lists all internal and external technologies that are thought to be important for the business (Salleh, Janczewski, & Beltran, 2015). The organizational factors make up the second construct. This relates to various traits that characterize a firm generally, such as firm size and communication procedures (Teo, Ranganathan, & Dhaliwal, 2006). The last construct discusses "the structure of the industry, the

presence or lack of technical service providers, and the regulatory environment" as examples of environmental factors (Baker, 2012). As highlighted in Figure 5 below, the TOE framework will be used as a guideline to explore the different factors when adapting to information security compliance in this study explained below.

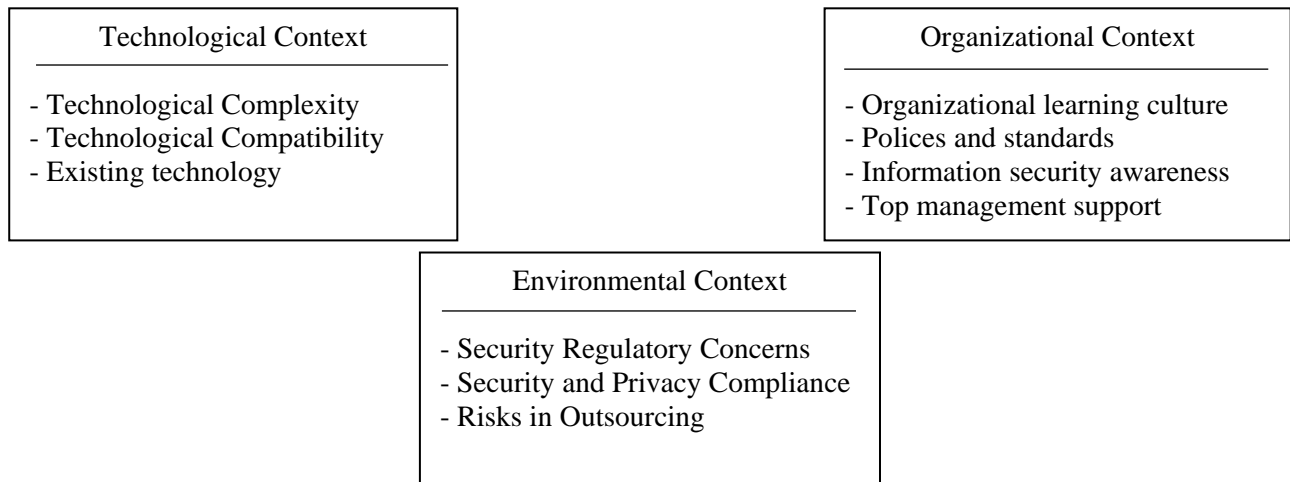


Figure 5: Identified security and privacy challenges (Source: Salleh & Janczewska, 2016)

2.6.3.1 Technological factors

Technological factors can be defined as the “internal and external technologies” that are used by the organization (Battistella, De Toni, & Pillon, 2016). According to Baker (2012), technological factors are all relevant existing technologies in an organization that is already in use and the available technologies in the marketplace that are not used by the organization. The author further elaborates that, technological innovations that are not used by the organization can influence the way organizations perceive innovations by showing how the technology can enable them to evolve and adapt positively.

2.6.3.1.1 Technological Compatibility

The definition of "compatibility" is the perceived alignment between a company's current security controls and technology and the security requirements (Salleh & Janczewska, 2016). According to Rogers' (2003) notion of compatibility, an invention is compatible to the extent that it satisfies the needs, requirements, and values of a potential adopter (Matandela, 2017). Traditionally it has been argued that the opposite is also true, namely, that compatibility issues with internal information

systems applications might prevent innovations from spreading further (Cooper & Zmud, 1990). The compatibility factor has frequently been seen to have an impact on the adoption of new technologies in earlier studies on technology adoption (Borgman, Bahli, Heier, & Schewski, 2013). Over the past ten years, the compatibility of security technologies and policies in safeguarding different corporate systems, hardware, and software has increased (Hashem, Yaqoob, Anuar, & Mokhtar, 2015). Therefore, the likelihood that an organization will accept the solutions will be higher when they think that their current security technology and controls are compatible with the security criteria.

2.6.3.1.2 Existing technology

According to Moghavvemi, Salleh, Sulaiman, & Abessi (2015), Existing technology is the interaction of a company's projected technical innovation and its current technological environment. The authors further state that this will also be one of the factors influencing the choice to adopt technological innovation. Another author describes existing technology as within an organization that establishes the limits of how much technology adoption can make (Baker, 2012). It is insufficient for an organization to solely rely on its technological resources. In addition, a company needs creative, knowledgeable employees who can keep it one step ahead of its competitors in terms of technology. (Metaxiotis, 2009).

2.6.3.1.3 Technological Complexity

Techno-complexity is a property of information technology that causes individuals to feel underqualified (Hwang & Cha, 2018). According to the author's claims, techno-uncertainty is the term used to describe the uncertainty in technology as a result of ongoing changes and improvements in computer hardware and software. For new technologies to be adopted more widely, they must be simple to use (Alshamaila, Papagiannidis, & Stamati, 2013). Rogers (2003), "describes complexity as the degree to which an innovation is seen as being particularly challenging to grasp and apply". As Rogers also stated, complexity is adversely connected with the rate of adoption, in contrast to the other qualities (Sahin, 2006). Therefore, an innovation's excessive complexity is a major barrier to adoption.

2.6.3.2 Organizational factors

Leung, Lo, Fong, & Law (2015), defines organizational factors as "the characteristics and resources available to the firm to successfully adopt and operationalize the new technology". In addition, an organization must have all the necessary resources in place to adapt to or with an innovation or

technology. Baker (2012), argues that organizational factors influence adoption and implementation decisions in a wide range of ways. Structures should be linked to organizational factors between employees, organizational communication processes, firm size, and the number of slack resources. Additionally, larger organizations are more likely to adopt new technologies because they have access to more financial and human resources, which increases their capacity to support and effectively operationalize the adoption of new technologies (Tornatzky & Fleischer, 1990).

2.6.3.2.1 Organizational learning culture

The qualities and orientation of an organization toward learning, particularly when it comes to the adoption of sophisticated technologies, are referred to as organizational learning culture (Ahmad Salleh, Janczewski, & Beltran, 2015). Odor (2018), states that any organization's ability to adapt to environmental changes, accept change, and improve its operations is crucial to its existence. This is true, especially for profit-oriented organizations. According to Islam, Khan, Ahmad, & Ahmed (2013), the organization's learning culture is a critical component to improving workers' favourable work-related attitudes and behaviours. Furthermore, it is known as a shift in the knowledge base of an organization brought on by prior experience (Leithwood & Louis, 2021). A consequence or by-product of organizational learning, which takes a sophisticated and multifaceted approach, has been referred to as learning organizations (Odor, 2018).

2.6.3.2.2 Information security awareness

The benefit of adhering to information security standards and procedures is referred to as organizational security culture by different personnel (McIlwraith, 2006). One strategy to increase information security compliance is to implement information security awareness programs, which can increase users' knowledge of and understanding of security procedures and mechanisms within businesses (Puhakainen & Siponen, 2010). Bulgurcu, Cavusoglu, & Benbasat (2010), for example, point out that the existence of information security awareness programs has a significant impact on employees' perceptions of the advantages of compliance and the costs of non-compliance. Alhogail & Mirza (2014), stated that the organization's values, beliefs, and knowledge, which convey the idea that information security is everyone's duty, shape the information security culture. Information security should be integrated into organizational culture and ethical standards, and it should be a part of every action undertaken by senior management and all personnel (Chen, Chau, & Li, 2018).

2.6.3.2.3 Top Management support

Senior management's initiatives to enhance information security compliance are the basis of management commitment (Kajava, Anttila, Varonen, Savola, & Rönning, 2007). It may be possible to assess management commitment by looking at how employees view management's efforts to achieve information security compliance as evidenced by “management support and involvement”, “goal alignment” and “effectiveness” (Knapp, Marshall, Rainer, & Ford, 2006). The choices, investments, and actions made to enforce information security rules throughout the firm can also be referred to as management support (Lee, Lee, & Yoo, 2004). The authors go on to say that senior management's involvement in addressing the organization's information security challenges is a sign of management involvement. In public organizations, the adoption of information security compliance is influenced by management commitment (Smith & Jamieson, 2006).

2.6.3.2.4 Information security policies and standards

The ability of an organization to foster a culture in which its personnel follows the rules, procedures, and technical controls that are outlined in its information security policies (ISPs) is crucial to effective information security management (Fazlida & Said, 2015). Information security policy is when management wants the employees to abide by the intentions, principles, regulations, and guidelines (Somestad, Hallberg, Lundholm, & Bengtsson, 2014). The goal of the information security policy is to "give management direction and support for information security," as stated clearly by ISO/IEC, 2009 (Abusef & Tarofder, 2021). It should outline information security responsibilities, permissible use of computer resources, the penalties for breaking security policies, and the appropriate training for various sorts of personnel (Ifinedo, 2012).

2.6.3.3 Environmental factors

The TOE framework's environmental context refers to the region and setting in which the organization operates concerning its sector, its competitors, its suppliers, and the government (Tornatzky & Fleischer, 1990). The environmental factors include industry characteristics, competitor intensity, market structures, government regulations, etc. According to Baker (2012), “the environmental factors include the structure of the industry, the presence or lack of technical service providers, and the regulatory environment”. Hence, the environmental context in the TOE framework can have favourable or non-favourable effects on IT adoption within an organization. For instance, certain industries, like the information technology and communications sectors, would be quicker to adopt new technology than others, like the retail sector, which is less accustomed to it (Kashi, Zheng, & Molineux, 2016).

2.6.3.3.1 Security and privacy compliance

Solid administrative, technical, and physical security measures are used by privacy-compliant organizations to guarantee the confidentiality, integrity, and availability of data (Thomson Reuters, 2021). This involves having the capacity to recognize and stop unauthorized or improper access to data (Tabrizchi & Rafsanjani, 2020). To address emerging risks, information security must be evaluated, tracked, and updated continuously (Coderre & Police, 2005). There must be a tight set of guidelines and regulations for data sharing (Pasquier, Singh, Evers, & Bacon, 2015). The compliance method is essentially a security management strategy that entails establishing a security management system that complies with standards and then having that system's compliance with the standards audited (Mitchell, 2015). The author further asserts that the fundamental benefit of such a strategy, according to the author, is that it promotes the widespread adoption of accepted best practices for IT security.

2.6.3.3.2 Security and privacy regulations concerns

Organizational worries about assuring compliance with security and data privacy rules are referred to as "security and privacy regulatory concerns" (Burmeister, Drews, & Schirmer, 2019). Traditional data protection laws were primarily developed and implemented based on the idea that structured data is easier to maintain and evaluate to ensure its appropriate use (Cumbley & Church, 2013). The vast volume of unstructured data that enterprises must work with may make it difficult for them to fully comply with rules, which is something that the majority of organizations would want to do (Kim, Yang, & Park, 2014). For example, privacy laws and regulations in the EU are typically regarded as being tougher than those in other countries (Pearson & Benameur, 2010).

2.6.3.3.3 Risk of outsourcing

The term "risks of outsourcing" refers to the potential security and privacy issues that may arise when an organization chooses to outsource its security or uses third-party security products (Ahmad Salleh, Janczewski, & Beltran, 2015). As a result, enterprises may need to use outsourcing techniques for all or a portion of their data environments (Jagadish, et al., 2014). Risks related to security will arise from an organization's reliance on service providers and outside tool vendors (Ahmad Salleh, Janczewski, & Beltran, 2015). This is demonstrated by numerous studies that indicated that firms planning to outsource their IT infrastructure and technologies are more concerned about security concerns (Nassimbeni, Sartor, & Dus, 2012). The limitation of the security structure leads to dependence on third-party tool vendors and service providers, among other things (Kshetri, 2014).

Even if outsourcing is essential to producing and monetizing data and information, it will necessitate additional security and privacy considerations (Chen, Mao, & Liu, 2014).

2.7 Chapter Summary

The chapter starts by introducing the literature review in **Section 2.1**. **Section 2.2** gives an overview of Small-medium enterprises by defining the term SME, discussing the role of SMEs in South Africa as well as what challenges SMEs face. **Section 2.3** conceptualizes the term information by providing a clear definition of information and the importance of information in organizations today. **Section 2.4** provides an introduction to information security also known as InfoSec is provided by discussing the definitions of InfoSec, InfoSec principles (named the Confidentiality, Integrity, and Availability triad), InfoSec policies and standards, and lastly, InfoSec controls named the administrative, physical, and technical controls. **Section 2.5** looks at InfoSec governance. A brief overview of what InfoSec governance entails was given followed by an introduction to the first governance called King IV. Then, the Electronic Communications and Transactions (ECT) Act was discussed followed by the Protection of Personal Information (POPI) act. The last section which is **Section 2.6**, discusses the InfoSec theories and frameworks. One theory was discussed called the Institutional theory where the three forces of the theory were discussed as the effectiveness of the theory. Then, two frameworks were discussed called the National Cybersecurity Policy Framework and the Technological-Organizational-Environmental framework. The T-O-E framework was used to guide this study by identifying potential factors that influence InfoSec Compliance among SMEs. The following chapter is called the research methodology and it covers all the research methods, research design, and research strategies used in this study.

Chapter 3: Research Methodology

3.1 Introduction

In the previous chapter, titled the literature review, the researcher focused on existing literature that discusses the research topic and the main question. Chapter 3 presents the research methodology and design that was used to answer the research questions and reach the research objectives. According to Al Kilani & Kobziev (2016), “research methodology is useful to establish the structure of research, such as strategy, approach, research philosophy, and components of the methodology”. However, this idea is more easily connected with method than with methodology. In an information systems context, a research methodology can be seen as an overall strategy for conceptualizing, conducting, and developing scientific knowledge. As a result, the research methodology explains and defines the study's objectives while also identifying the conditions needed to meet those objectives (Ziemba, Papaj, & Zelazny, 2013). The research methodology for this study was guided by the research onion structure that was first developed in 2007 by Saunders, Lewis, and Thornhill. In an illustration of the latest research onion (2019), the authors presented the different stages when developing knowledge during a research study.

Chapter 3 is outlined as follows. Section 3.2 presents the research onion framework by Saunders, Lewis, and Thornhill (2019). As a sub-section of the research onion, section 3.2 is supported by the rationale for using the research onion framework in section 3.2.1. The research philosophy is covered in section 3.3, the research approach in section 3.4, and the methodological choice in section 3.5. Then, the research strategy is presented in section 3.6 followed by the research time horizon in section 3.7. Section 3.8 focuses on the data collection for this study, with the data analysis in section 3.9. Lastly, the chapter concludes with ethical considerations in section 3.10 followed by a summary of the chapter in section 3.11.

3.1.1 The research onion framework

The research onion was first developed by authors Saunders, Lewis, and Thornhill in the year 2007. It illustrates different stages that need to be followed when developing a research strategy and methodology when conducting research. According to the authors, “each layer in the onion describes a detailed stage of the analysis process” (Saunders, Lewis, & Thornhill, 2007). It can be seen as giving a researcher an effective progression while designing a research methodology. It is also seen as valuable because it may apply to any studying approach and in a variety of contexts.

For this study, the author emphasizes the research onion as a guide for this research to developing an efficient research methodology by following each stage of the onion as shown in Figure 6 below. The authors outline six steps that a researcher must complete to create a successful research methodology. The first stage describes the research philosophy that requires definition. This can be considered as a starting point in the onion, followed by the next stage named the research approach. The third stage is the methodological choice and the fourth stage is the research strategies also known as the research design. The fifth stage provides the time horizon of the research strategy and the last step presents the techniques and procedures when data collection and analysis take place.

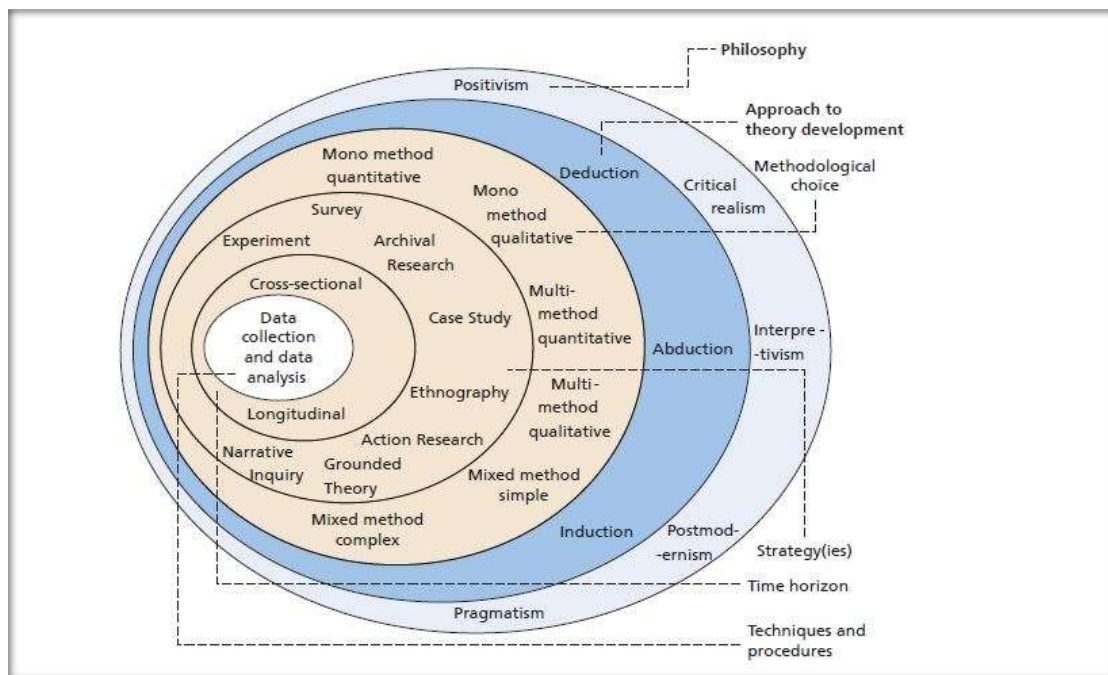


Figure 6: Research onion (Source: Saunders, Lewis, & Thornhill, 2019)

3.1.2 The rationale for using the research onion

The motivation for using this framework during this study is that the framework helps the researcher to understand the series of stages under different methods of data collection as well as illustrates steps for methodological studies. Benefits of using the research onion include: “It is a useful tool for thinking holistically about methodology” (Thesismind, 2019), as well as “it can be effectively adapted to different models” (Research Onion - Explanation of the Concept, 2018). Using the research onion framework, made it possible to not leave out any information on what techniques and methods were

used during this study. Each chosen stage by the researcher in the research onion can be considered useful if followed effectively during a study. These stages are described in more depth below.

3.2 Research Philosophy: Positivism

In research, “it is important to understand and articulate the nature of reality, what is out there and how to get the knowledge thereof” (Rehman & Alharthi, 2016). These are considered the elements of research paradigms. A paradigm can be defined as “a basic belief system and theoretical framework with assumptions about ontology, epistemology, methodology, and methods” (Rehman & Alharthi, 2016). In other words, it pertains to how we perceive and analyze the world as it is. Another author describes research paradigms as research philosophies that are used as “academic discipline and part of the broader canon of the humanities” (Hassan, Mingers, & Stahl, 2018). Thus, from a university context, the student will be taught the different types of philosophies in research.

For a particular study to be carried out successfully, a researcher should comprehend the following research paradigms. Each research paradigm comprises its theoretical assumptions based on five key theories namely how reality exists and what can be known about it (ontology), how knowledge can be acquired (epistemology), roles of value (axiology), how the world should be studied (methodology) and what the techniques will be to study a specific methodology (methods). These terms are defined in Table 4 below.

Table 4: Definitions of key research paradigms (Sources: Saunders, Lewis, & Thornhill, 2019)

Theory:	Definition:	Source:
Ontology	“assumptions about the nature of reality”	(Kaushik & Walsh, 2019)
Epistemology	“the nature and forms of knowledge”	(Scotland, 2012)
Axiology	“the nature of ethics and what we value”	(Biddle & Schafft, 2015)
Methodological	“how to go about it”	(Ugwu, Ekere, & Onoh, 2021)
Rhetorical	“A way to understand and account for the way any kind of human symbol use functions in any realm.”	(Foss, Foss, & Trapp, 2002)

According to Saunders, Lewis, & Thornhill (2019), a set of views and presumptions about how knowledge is developed constitute research philosophy. More specifically, it will involve the development of knowledge in a particular field. There will be assumptions and beliefs that a researcher will have during the different stages of research in their field. In addition, research philosophy describes different assumptions on how a researcher views and sees the world. All the research-related presumptions, background information, values, and experiences go under this category (Fugard & Potts, 2015). How a researcher sees and views the relationship between knowledge and the research process will have a significant influence on what philosophy is adopted.

This research study falls in line with the positivism research paradigm. According to Antwi & Hamza (2015), “the positivist research paradigm underpins a quantitative methodology”. Another author describes positivism as “the philosophical stance of natural scientists that are working with observable reality within society leading to the production of generalizations” (Alharahsheh & Pius, 2020). Therefore, positivism is concerned with the discovery of truth and the presentation of it through empirical means.

3.3 Research Approach: Deduction, Inductions, and Abduction

The second stage in the research onion refers to the research approach. A research approach is a strategy and procedure that incorporates broad hypotheses with specific data gathering, analysis, and interpretation (Goundar, 2012). The research onion emphasizes the importance of how far the development of your research can go through theory testing or theory development. This is presented through three approaches that can be adopted named inductive, deductive, or abductive approaches as described in Table 5 below.

Table 5: Deduction, induction, and abduction (Source: Saunders, Lewis, & Thornhill, 2019)

	Deduction	Induction	Abduction
Logic	“The premises are true, the conclusion must also be true”.	“Known premises are used to generate untested conclusions”.	“Known premises are used to generate testable conclusions”.
Generalisability	“Generalizing from the general to the specific”.	“Generalizing from the specific to the general”.	“Generalizing from the interactions between the specific and the general”.
Use of data	“To evaluate propositions or	“To explore a phenomenon,	“To explore a phenomenon, identify

	hypotheses related to an existing theory”.	identify themes and patterns, and create A conceptual framework”.	themes and patterns, locate these in a conceptual framework and test this through subsequent data collection, and so forth”.
Theory	“Theory falsification or Verification”.	“Theory generation and building”.	“Theory generation or modification; incorporating existing theory where appropriate, to build new theory or modify the existing theory”.

To answer the research question and meet the research objectives, a deductive approach was used during this study. The deductive researcher, according to Creswell & Plano Clark (2007), "works from the 'top-down,' from a theory to hypotheses to data to confirm or deny the theory". The deductive approach employs a theme-based structuring framework for the coding process (Vaismoradi, Turunen, & Bondas, 2013). The framework sometimes referred to as a start list, is utilized in the analysis to guarantee that some fundamental notions are present in the data (Thomas, 2006). “Initial codes are generated from existing literature on the topic of inquiry or what is known about the phenomenon of inquiry using the deductive approach, which is supported by the research aims, research questions, and interview questions” (Azungah, 2018). The deductive approach is also associated with quantitative research, “where data are collected and analyzed to test theory” (Saunders, Lewis, & Thornhill, 2019). This is discussed in the next section.

3.4 Methodological Choice: Quantitative research design

The third stage in the research onion presents the methodological choice. This stage provides all the methodological choices for research design. According to Saunders, Lewis, & Thornhill (2019), a research design can be described as “the general plan of how a researcher will go about answering the research questions”. The authors further state that the research design “will contain clear objectives derived from the research questions while specifying the source or sources from which data collection will be done and how it will be collected and analysed”. Furthermore, a discussion about ethical issues and constraints will also be discussed as part of the research design. The research onion provides three methodological choices named the quantitative, qualitative, and mixed methods research design to achieve coherence during a research study as demonstrated in Figure 7 below.

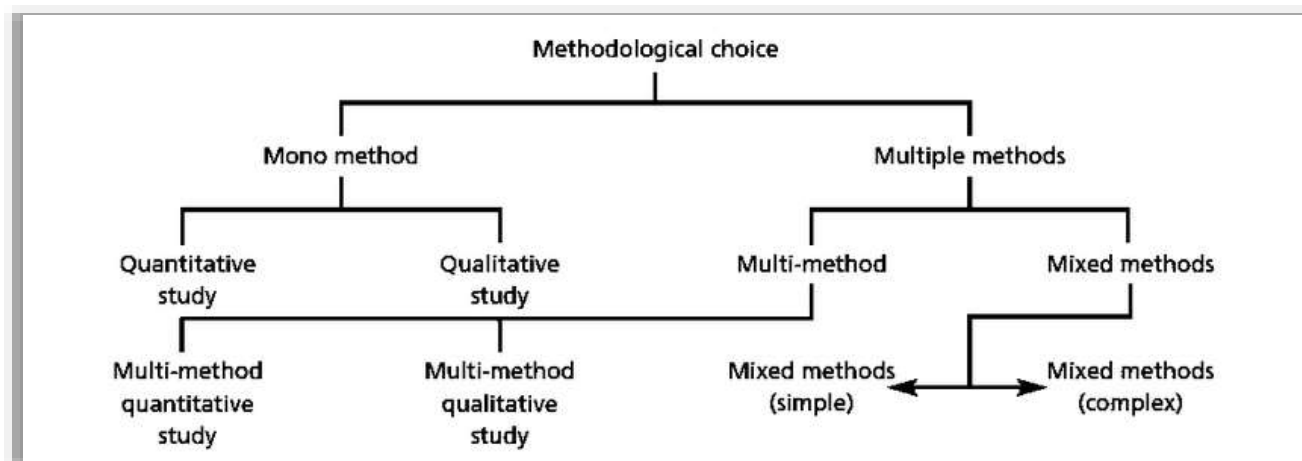


Figure 7: Methodological choice (Source: Saunders, Lewis & Thornhill, 2016, p.167)

This study used the quantitative research design as the methodological choice together with the mono method. Quantitative research design is typically linked with the positivism research philosophy especially when a researcher uses ‘predetermined’ and ‘highly structured’ data collection methods and techniques (Saunders, Lewis, & Thornhill, 2019). The research onion claims that positivism, the deduction method, and quantitative research design are all exclusively linked. According to Apuke (2017), quantitative research involves assessing and quantifying variables to construct findings. The author further states that quantitative research entails using and analyzing numerical data using particular statistical methods to respond to queries like "who, how much, what, where, when, how many, and how". During this study, the author used primary numerical data to answer the research questions while using surveys to collect the data. Quantitative research design may use singular data collection methods such as surveys and questionnaires. This is known as the mono method and is used in this study.

3.4.1 Unit of analysis

There are no restrictions on what can be studied, who can be studied, or the units of analysis in social research. According to Babbie (2021), units of analysis refers to “what” and “whom” being studied. This includes individuals, groups, and non-human entities. Another author describes the unit of analysis as “the group about which information is collected and analyzed” (Sedgwick, 2014). As a result, the unit of analysis is anything the researcher wants to investigate to generate a summary description of all of these units and explain their differences. According to another author, the units of analysis are “the most important part of any research as the whole research is based upon the unit

of analysis” (Khan, 2014). Moreover, it determines the boundaries of what is studied or disregarded within the study and is what the data are about for the goal of addressing the research problem (Ritella, Rajala, & Renshaw, 2020). The unit of analysis for this study will be organizations. The specific unit of analysis is small-medium enterprises (SMEs) in Cape Town. This was considered to be the appropriate unit of analysis to determine where SME’s employees and managers are in terms of protecting their information and being prepared for information security compliance.

3.5 Research Strategy: Survey

The fourth stage in the research onion describes the research strategy during a study. The research strategy refers to “provides the overall direction of the research including the process by which the research is conducted” (Wedawatta, Ingirige, & Amaratung, 2011). The research onion explores different types of research strategies that can be used to answer research questions during the development of a study. Some of those strategies include experiments, surveys, case studies, etc. For this study, the researcher used the survey strategy to collect the data to answer the research questions.

This study used a survey strategy to collect primary data. “A survey can be defined as a procedure where data is systematically collected from a specific sample of a population through any form of direct solicitation, such as interviews, telephonic interviews, or email questionnaires” (Mathiyazhagan & Nandan, 2017). According to Levy & Lemeshow (2013), a survey generally includes two steps. The first step includes developing a sampling plan that will be used as a methodology to select a sample from a specific population. “The sampling plan describes the approach that will be used to select the sample, how an adequate sample size will be determined, and the choice of media through which the survey will be administered” (Glasow, 2005). The second phase entails the method for estimating the population using sample data and determining the accuracy of those population estimates (Levy & Lemeshow, 2013). During this process, the required response rate and survey accuracy are determined (Dillman, Smyth, & Christian, 2014). The motivation for using a survey strategy for this research is that a survey is a good way for reaching a metric or statistic as a tool to demonstrate patterns, relationships differences as well as trends through a breadth of data.

This strategy is mostly associated with the deductive research approach when it comes to the collection of data. Surveys are most effective when it comes to the ‘who’, ‘what’, ‘where’, and ‘how’ questions which are done through exploratory and descriptive research (Nardi, 2018). It allows the researcher to sample a representative portion of a population in which case this study was small-

medium enterprises situated in Cape Town. Using a survey strategy allows for the collection of standardized data from large sample sizes for statistical analysis. The sample size for this study was 200 SMEs which allowed the observation of their employee’s subjective perspectives when it comes to information security adoption. The views and opinions of these employees allowed the researcher to understand their behaviour in the business environment from their perspective.

3.6 Research time horizon: Cross-sectional

The research onion discusses two types of time horizons named longitudinal and cross-sectional timing. According to Saunders, Lewis, & Thornhill, (2019), a longitudinal study refers to the ability to study change and development. In addition, the authors state that it will “provide you with a measure of control over some of the variables being studied”. Although the challenge of time may be a concern, a researcher can introduce a longitudinal element in their research. This research was not a longitudinal study. The second time horizon is Cross-sectional timing. This timing refers to conducting a research study of a particular phenomenon at a particular time. It allows sufficient time for a researcher to conduct a study. This study made use of the cross-sectional timing horizon and is discussed below.

This research used cross-sectional timing to complete the survey strategy in 10 weeks. In Table 6 the weeks are shown by all the activities that were carried out for each week. This allowed the researcher to keep track of how many weeks each activity will take to reach the objectives of this study. In addition, the unit of analysis for this study was organizations. The specific unit of analysis was Small-medium enterprises (SMEs) in Cape Town, Western Cape. This was considered an appropriate unit of analysis to determine where SMEs’ employees and managers are in terms of protecting their information and being prepared for information security compliance.

Table 6: Weekly timeline of survey strategy

Duration:	Activities:
Week 1	1. Develop a research sample.
Week 2-4	2. Engage with targeted respondents to obtain informed consent.
Week 5-10	3. Distribution of survey questionnaires to targeted respondents.
Week 11	4. Collection of surveys.
Week 12-15	5. Data analysis and interpretation.

Week 16-17	6. Revise and edit the thesis draft.
Week 18	7. Submit draft to supervisor.
Week 19	8. Revision and edit for final submission.
Week 20	9. Submission of the final thesis to relevant committees.

3.7 Data Collection

Data collection is considered important for statistical analysis. Kabir (2016), defines data collection as “the process of gathering and measuring information on variables of interest, in an established systematic fashion that enables one to answer stated research questions, test hypotheses, and evaluate outcomes”. The author further asserts that any data collection should aim to gather high-quality data that can be used to create comprehensive data analyses and build convincing arguments in support of the questions being posed. This section of the research study aims to present all the data collection techniques that were used to answer the research questions and objectives.

3.7.1 Population

The following steps as described by Taherdoost (2016) were used in this study to ensure the correct population and sampling methods were used to answer the research questions and objectives.

3.7.1.1 Step one: Define the target population

Several items, units, or subjects fall under the reference of a study, referred to as a population. Populations can be composed of finite or infinite units (Agarwal, 2007). Ideally, it would be better to analyze every individual within the population for the actual condition of learning achievements subject-wise, but most of the time, it is impossible to achieve this by studying the entire group (Bhatt, 2020). The study population included organizations such as small and medium enterprises. The population included SMEs that are located in Cape Town in the Western Cape region.

3.7.1.2 Step two: Choosing a sampling technique

In research, a sample refers to “a group of people, objects, or items that are taken from a larger population for measurement” (Taherdoost, 2016). For a researcher to extrapolate the sample's results to the entire population, the sample must accurately reflect the population (Ishak & Abu Bakar, 2014). As a result, the goal of sampling is to draw conclusions about populations from samples by utilizing inferential statistics to ascertain the features of a population. (Levy & Lemeshow, 2013).

According to Dörnyei (2007), “Convenience sampling is a type of nonprobability or nonrandom sampling where members of the target population meet certain practical criteria, such as easy accessibility, geographical proximity, availability at a given time, or the willingness to participate is included for the study”. Additionally, it refers to research subjects from the population who can easily be reached by researchers (Given, 2008). In convenience sampling, the researcher collects data from individuals who are easy to reach, such as recruiters attending a staff meeting to participate in the study (Etikan, Musa, & Alkassim, 2016). Since the study chose to use SMEs that are easily accessible and within the researcher's geographic reach, this type of sampling was deemed most suitable.

3.7.1.3 Step three: Collecting data

The sampling process included selecting specific SMEs that met the criteria set for this research study. The criteria include an SME that has been established for more than 5 years, preferably from 2013 to 2021. Secondly, the business should have more than 25 employees trading in any industry. The last and most vital criteria are that the chosen SME should have an IT infrastructure that includes physical components like computers and network facilities.

3.7.1.4 Step four: Assessing the response rate

The response rate was assessed through google forms on a weekly basis. Over 300 surveys were distributed and 120 responses were received. The sample size where 200 respondents and 120 surveys were completed correctly.

3.7.2 Primary data

Primary data can be collected through interviews, experiments, surveys, observations, etc. Information can be gathered using a variety of techniques, and these techniques can be divided into two categories: primary data and secondary data. “Primary data refers to data that is being collected for the first time by a researcher while secondary data is already collected and used by others” (Ajayi, 2017). The difference between the two types of data can be distinguished by looking at primary data as “factual” and “original” while secondary data can be considered as the “analysis” and “interpretation” of the primary data (Hox & Boeije, 2005). The difference between the two types of data is discussed in Table 7 below.

Table 7: Primary data vs Secondary data (Source: Ajayi, 2017)

Concept	Primary data	Secondary data
1. Definition	Known as "first-time" data, they were gathered by the researcher themselves.	Referred to as past data that was gathered by another party.
2. Data	"Real-time data"	"Past data"
3. Process	High involvement	Simple and quick
4. Source	Surveys, experiments, interviews, etc.	Journal articles, websites, books, etc.
5. Cost-effectiveness	Expensive	Economical
6. Collection time	Long	Short
7. Specific	Suited to the needs of the researcher	It may or may not be tailored to the demands of the researcher
8. Available	Rough shape	Enhanced shape
9. Accuracy and reliability	More	Less

3.7.3 Instrument development: Survey

The instrument development for this research study was survey questionnaires. The instrument was designed by developing a clear question structure that was divided into three categories. The three categories included the Technological, Organizational, and Environmental sections. This was influenced by the Technological-Organizational-Environmental (TOE) framework developed by Tornatzky and Fleischer's "the process of technological innovation" in 1990. Multiple choice questions were used as they are considered intuitive, easy to use in different ways, help to produce easy-to-analyze data, and provide the respondents with mutually exclusive choices (Brace, 2004). The multiple-choice questions were presented with a statement by answering as a Likert scale of strongly agree to strongly disagree options. The survey questionnaire was short and to the point but also ensured it is consistent with the research objectives. The different sections of the survey questionnaire are discussed below.

3.7.3.1 Section 1: Biographical details

This section of the survey required the participant's details such as the organization's name, contact details, position at the organization, and how long the participant is currently working at the organization.

3.7.3.2 Section 2: Technological factors

This section of the survey was related to questions that were based on a technological perspective. The questions covered technological compatibility, technological complexity, policies and standards, and existing technology in an organization.

3.7.3.3 Section 3: Organizational factors

This section of the survey was related to questions that were based on an organizational perspective. The questions covered organizational learning culture, information security culture, and top management support.

3.7.3.4 Section 4: Environmental factors

This section of the survey was related to questions that were based on an environmental perspective. The questions covered security and privacy compliance, security and privacy regulatory challenges, and risks of outsourcing.

3.7.4 Survey questionnaire: Validity and Reliability

In social sciences, survey questionnaires are one of the most widely used data collection instruments. “The main objective of a survey questionnaire in research is to obtain relevant information most reliably and validly” (Taherdoost, 2016). Therefore, reliability and validity are considered significant aspects when it comes to research methodology as it relates to the accuracy and consistency of the survey questionnaire. Another author describes reliability and validity as “the two most important and fundamental features in the evaluation of any measurement instrument or tool for good research” (Mohajan, 2017). The researcher goes on to describe the survey questionnaire's reliability and validity in more detail below.

3.7.4.1 Construct validity

Construct validity is “the degree to which evidence about a measure’s scores supports the inference that the construct has been appropriately represented” (Polit, 2015). This study practiced construct validity by making sure that all respondents received a detailed information sheet before giving their consent to partake in this research study. The information sheet included all the necessary information about the study like the study title, the background of the author, the purpose of the study, etc. All respondents had the option to decline or withdraw from partaking in the study at any given time. After

consent was given by the respondents the survey questionnaire was shared. The author made sure that the survey questions were accurately measured. The following steps were used to ensure data validity during the collection process.

3.7.4.1.1 Steps to data validity:

- I. The survey questionnaires were only shared with SMEs based in Cape Town,
- II. The time to complete the survey questionnaire was stipulated,
- III. The survey questions were pre-tested and pilot-tested before sharing with respondents.

3.7.4.2 Pre-testing

After the draft of the survey questionnaire was completed, the author completed a pretesting before finalizing the survey. Pre-testing is the only way for researchers to ascertain the meaning attached to survey questions "before it's too late," that is before a significant correction is made to the incorrect questions or to the questions about which the researcher is doubtful (Bowden, Fox-Rushby, Nyandieka, & Wanjau, 2002). During this study, the researcher conducted a pre-test survey questionnaire with one of the SMEs in Cape Town, where the head of IT and the receptionist agreed to participate in the survey to provide feedback to the researcher. The given feedback enabled the researcher to determine if the questions were flawed or if any errors were present. Moreover, the researcher could assess whether the questions were difficult, easy, or repetitive and if they related to the purpose of the study.

3.7.4.3 Pilot-Testing

To ensure data validity, a pilot test was done after the pre-testing process. The following steps were followed to ensure an accurate pilot test:

- Pilot subjects – The researcher received permission to administer the survey questionnaire to an SME before the study was conducted to receive feedback on the survey questionnaire time, questions, and layout. The survey questionnaire was received by the administrator receptionist and IT manager.
- Feedback – Feedback was given to the researcher on all the difficult questions and the time to complete the survey questionnaire.
- Survey questionnaire time – The author decided to limit the time to complete the survey questionnaire by revising longer questions and shortening them so that the participant can read the questions more quickly.

- Difficult questions – The researcher discarded all difficult and unnecessary questions in the survey questionnaire which made the time to complete the questionnaire shorter.

3.7.5 Reliability

Reliability refers to the degree of assurance that may be put in the information obtained by using an instrument (Alshenqeeti, 2014). It displays how error-free (bias-free) the instrument is, ensuring accurate measurement across time and among all of the instrument's many parts (the observed scores) (Mohajan, 2017). Reliability in quantitative research relates to the consistency, stability, and repeatability of results; for instance, a researcher's finding is considered reliable if consistent results were obtained in a variety of circumstances that were comparable but not identical (Heale & Twycross, 2015). There are two types of reliability called stability and internal consistency reliability.

3.7.5.1 Internal consistency reliability

The degree of consistency with which data is gathered determines internal consistency reliability (Sharma, 2016). It establishes the equivalence of values acquired by different observers using the same instrument (Mohajan, 2017). The most often used measure of internal consistency, coefficient alpha (Cronbach, 1951), has become standard in research. According to John & Soto (2007), this is accurate in part because of how straightforward it is to quickly determine alpha whenever a multi-item scale is applied. Alphas are also commonly employed since influential literature claim that they are both essential and sufficient for determining dependability (McCrae, Kurtz, Yamagata, & Terracciano, 2011). The author of this study used a statistical program and Cronbach Alpha to measure the consistency of the survey questions and data. A more detailed explanation is given in Chapter 4 under section 4.4.

3.7.6 Disposal of data

The primary data was stored on a USB drive and safely stored by the supervisor. All hard copies of the survey questionnaires were kept safe in a secure locked cabinet to which only the researcher and the supervisor had access. All research data and material will be kept for a maximum period of 1 year after the thesis paper is completed. When the thesis paper is marked and graded all material will be disposed of. This includes all hard copies of the survey questionnaires, consent forms as well as captured data for analysis purposes. The primary data stored on the USB drive will be deleted and hard copies will be shredded or burned to permanently destroy any evidence.

3.8 Data Analysis

The methods for data analysis utilized in the study are described in this section of the research methodology. Using information or data to support your research's aims, objectives, and methods is known as data analysis (Frank & Todeschini, 1994). To find relevant information for sensible decisions, data analysis can also be described as cleaning, converting, and modeling data (Zhao, 2015). Data analysis aims to remove useful information from data and make decisions based on that knowledge (Calzon, 2020). This section will pinpoint all the steps followed when the researcher constructed the data analysis for this study.

3.8.1 Quantitative data

Quantitative data can be described as any information or data that can be measured or quantified (Goertzen, 2017). This comprises factual data in the form of numbers and categories. If the data can be counted or measured, it is quantitative in nature (Samuels, 2020). Quantitative data in the form of categories typically contains alternatives such as "how many," "how much," or your personal experience or opinion on a scale of strongly agree to strongly disagree (Dörnyei & Csizér, 2012). The research questions in this study were measured and analyzed using primary data from survey questionnaires.

3.8.2 Statistical analysis

Statistics can be described as “an academic subject that involves presenting, interpreting, and reasoning about summary quantities derived from data sets” (Samuels, 2020). Measures of dispersion like range and standard deviation as well as measures of intermediate values like average (also known as mean), mode, and median are examples of frequently used statistical values (Leech, Barrett, & Morgan, 2013). This study used a statistical program called SPSS for the data analysis process. “SPSS (Statistical Package for the Social Sciences) is a widely used program for statistical analysis in social science” (Bala, 2016). The statistical program assisted the researcher of this study to perform quantitative data analysis by using descriptive statistics.

3.8.3 The quantitative data analysis process

According to Ali (2021), quantitative data analysis can be described as a “systematic process of both collecting and evaluating measurable and verifiable data”. It focuses on surveys, questionnaires, secondary data, statistics, and measurement. It has a statistical framework for analyzing or

interpreting numbers (Ritter & Munoz-Carpena, 2013). The researcher of this study used the 5-step approach to quantitative data analysis by Samuels (2020) to describe the data analysis during this study which is discussed below.

- **Step 1: Research aims and questions**

The research aims and research questions were discussed in chapter 1 and were consistent with the research objectives of this study.

- **Step 2: Consistent data collection**

Samuels (2020), describes this step as the “where”, “how” and “how much”. This relates to the population and sampling of this study and was covered in Section 3.8 above.

- **Step 3: Data spreadsheet and coding**

This study used online survey questionnaires as means of data collection. The online survey questionnaires were downloaded from Google forms and converted into an Excel spreadsheet. The researcher cleaned the data by deleting all errors and incomplete surveys. Then, the naming of the columns took place to make the data more presentable, and a codebook was created to keep track of all the headings. The data was coded as numerical data from 0 to 5 using a coding technique and were labelled in the codebook.

- **Step 4: Descriptive analysis**

Quantitative data analysis was used to analyze the raw data through SPSS and was presented as tables, charts, summaries, and graphs.

- **Step 5: Formal interpretation and reporting**

The author interpreted and reported on the results of the descriptive statistics in the next chapter (chapter 4) to describe the data.

3.9 Ethical considerations

According to David & Resnik (2011), ethics can be defined as “norms for conduct that distinguish between acceptable and unacceptable behaviour”. In research, there are many different reasons why ethics is considered important. Three of these crucial motives are to advance the goals of research by pursuing the truth, to advance cooperative principles by being trustworthy, and to guarantee that a

researcher will always be held accountable for their findings (David & Resnik, 2011). Another author defines ethics as “the standards of behaviour that guide your conduct concerning the rights of those who become the subject of your work or are affected by it” (Bell, 2008). In addition, the authors mention that these standards of behaviour will be used as a guide by several influences while conducting research. Research ethics committees are also considered vital as they fulfill several objectives. These objectives include “a proactive role, such as developing an ethical code, and an educational one, such as disseminating advice about conducting research ethically” (Saunders, Lewis, & Thornhill, 2019).

For this research study, the researcher understood all the research ethics and objectives set by the research ethics committees. All ethics were fulfilled and the researcher was provided with ethics approval from the committee in July 2020 (Appendix A). The main ethical principle that was adhered to in this research study was to keep the identities of all respondents confidential. No respondents were harmed physically or psychologically during this research. Every participant was allowed to leave the study if they were uncomfortable in any way. All information gathered during this study was kept confidential and sealed in a cabinet that was only open to the researcher and the supervisor. Data will be disposed of and deleted once the final dissertation is marked and graded. The language used in this research was comprehensive and clear to all respondents. Prior consent was requested if there were a possibility or the need for any audio recording during this research study. Lastly, all respondents were treated fairly and objectively in this research.

3.10 Chapter Summary

Section 3.1 and 3.2: The researcher first started the chapter by introducing the research onion that was used as a guide to filling all the gaps in the research methodology. **Section 3.3:** Then, the researcher looked at all the research philosophies in social science and adapted the positivism research paradigm. **Section 3.4:** The next section focused on the research approach where the author discussed the deductive, abductive, and inductive approaches. The deduction approach was used during this study where the researcher motivates how it fits with the study’s research design. **Section 3.5:** The researcher introduced the methodological choice in section 5 where the quantitative research design was discussed in detail. The mono method was also chosen and discussed along with the unit of analysis for the study. **Section 3.6:** The next section covered the research strategy by introducing the survey strategy as a means to collect data for this study. **Section 3.7:** In the next section the research time horizon was discussed and two types of research time horizons were introduced. This study found the cross-sectional timing more fit for the study according to the time spent on data collection.

Section 3.8: Then, the next section focused on the data collection for this study by looking at the sampling techniques, discussing primary data, instrument development, reliability and validity of survey questionnaires, and the disposal of data. **Section 3.9:** This section discussed the data analysis for the study by starting by discussing quantitative data, statistical analysis, and the quantitative data analysis process. **Section 3.10:** The last section discussed the ethical considerations for the research study by looking at all the principles that were followed during data collection. The following chapter covers the research results and analysis obtained from applying the research methods, techniques, and analysis process discussed in this chapter.

4.1 Introduction

In the previous chapter called the research methodology, the researcher presented the research methodology and design used to answer the research questions and reach the research objectives for this study. In this chapter called the research results, the researcher will present the data analysis derived from the data collected and provide an understanding of the results. Kabir (2016), describes the research results as “the data are summarized, in other words, analyzed to provide information for testing the hypotheses”.

The chapter begins by presenting the survey responses (section 4.2) by indicating how many surveys were distributed and completed, the organization type, and what sector the organization operates in. The following section 4.3 covers the biographic information of the respondents by gender, length at the company, job position, and organization type. In section 4.4, the researcher describes the data used in this study by explaining how the surveys were answered by the respondents, how reliable each question was, the validity of each question, and if the data collected was normally distributed.

In section 4.5, the researcher presents result 1 (section 4.5.1), which is based on answering the first research question, which is “*What technological factors are impacting SMEs' adoption of information security compliance?*” In section 4.5.2, result 2 is presented, based on the second research question that is “*What organizational factors are influencing SMEs' adoption of information security compliance?*” The next section, which is section 4.5.3, presents result 3 based on the third research question, which is “*What environmental factors affect the adoption of information security compliance by SMEs?*”

The next sections focus on reaching the research objectives by looking at the relationship between the technological, organizational, and environmental factors. Furthermore, the researcher investigates if there is a significant relationship between the respondents' job positions and experience with information security compliance in the workplace. Then, a regression analysis was done in the next part, followed by practical recommendations to SMEs drawn from the research results and analysis. The chapter is concluded with a chapter summary at the end.

4.2 Survey response

A total of 200 surveys were distributed through email to 200 SMEs based in Cape Town for 12 months. A total of 125 surveys were received, where only a total of 120 were considered valid and 5 surveys had errors and were considered incomplete. The response of 120 surveys were collected and the data was used to conduct the data analysis for this study. The data collection was performed through social media by using Gmail and LinkedIn. The sample was collected by one respondent per SME, which represented the company by completing the survey honestly and effectively. The aim was to target respondents who work with the information and data of the company and also worked in the IT department or closely with employees in that department. The respondents were from 7 different types, as shown in Table 8 below. The table shows that each organization type received a total of 30, 40, and 10 surveys to be completed and sent back to the researcher.

Table 8: Survey distribution and collection by organization type

Type of organization	Sector	Distribution	Received	Valid	Percentage
Retail	Trade	30	20	20	67%
Technical	Service	30	16	16	53%
Health	Service	30	28	25	83%
Personal care	Service	30	10	8	27%
Law	Private	30	10	10	33%
Business services	Service	40	38	38	95%
Other	Other	10	3	3	30%
Total		200	125	120	60%

4.3 Biographic information of the respondents

The respondents were requested to enter their details in section A such as gender, length at the company, role at the company, and the organization type. This information was requested to assist the researcher in drawing a comparison between information security compliance in the workplace and to determine whether their personal information influences their position in answering the survey. Before completing the survey, the respondents received consent forms (Appendix C) and the information sheet (Appendix B) that provided them with a complete overview of what the study was about. Section A of the survey (Appendix D) captured the personal information of the respondents that were used to discuss the frequency and results in the next sections. The significance of including biographical details in a study is to identify all life history experiences that may have an impact on a person's present personality and behaviours (Wang & Song, 2022).

4.3.1 Gender of respondents

The purpose of requesting the gender of the respondents was to determine in which gender group the respondents of the survey fall and if there was a significant gender difference in small businesses. According to Figure 8 below, there was a 50% split between the female gender and the male gender of the respondents. Therefore, no majority of the two genders can be identified in this study. This is an indication that both males and females are likely to work in small businesses.

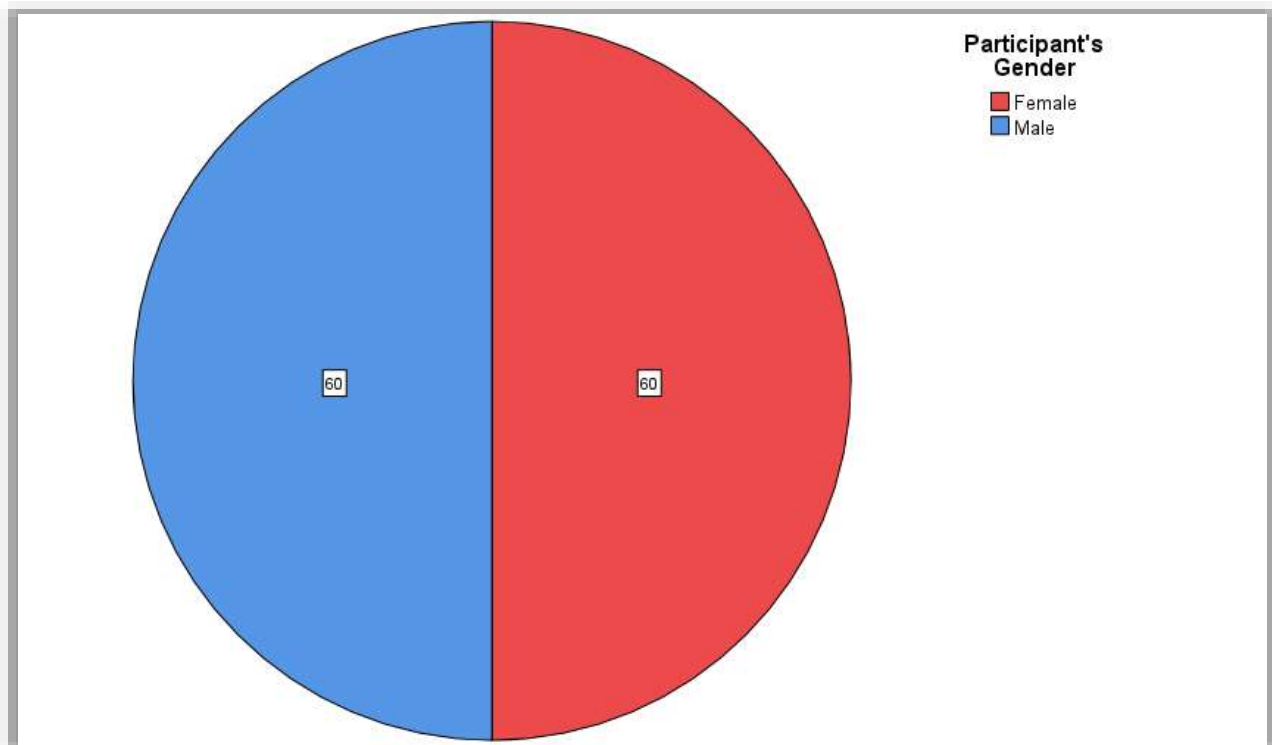


Figure 8: Respondent's gender

4.3.2 Length at company

The purpose of requesting the respondent's work experience at the company was to determine if their work experience has a significant impact on their information security compliance in the workplace. The results in Figure 9 below show that only 6 respondents work in SMEs for less than a year, a total of 67 respondents work at SMEs between a year and 5 years, 39 respondents work at SMEs for 5 to 10 years and only 8 respondents work in SMEs for more than 10 years. This is an indication that a majority of the respondents in this study have an experience of a year to 5 years working for small businesses.

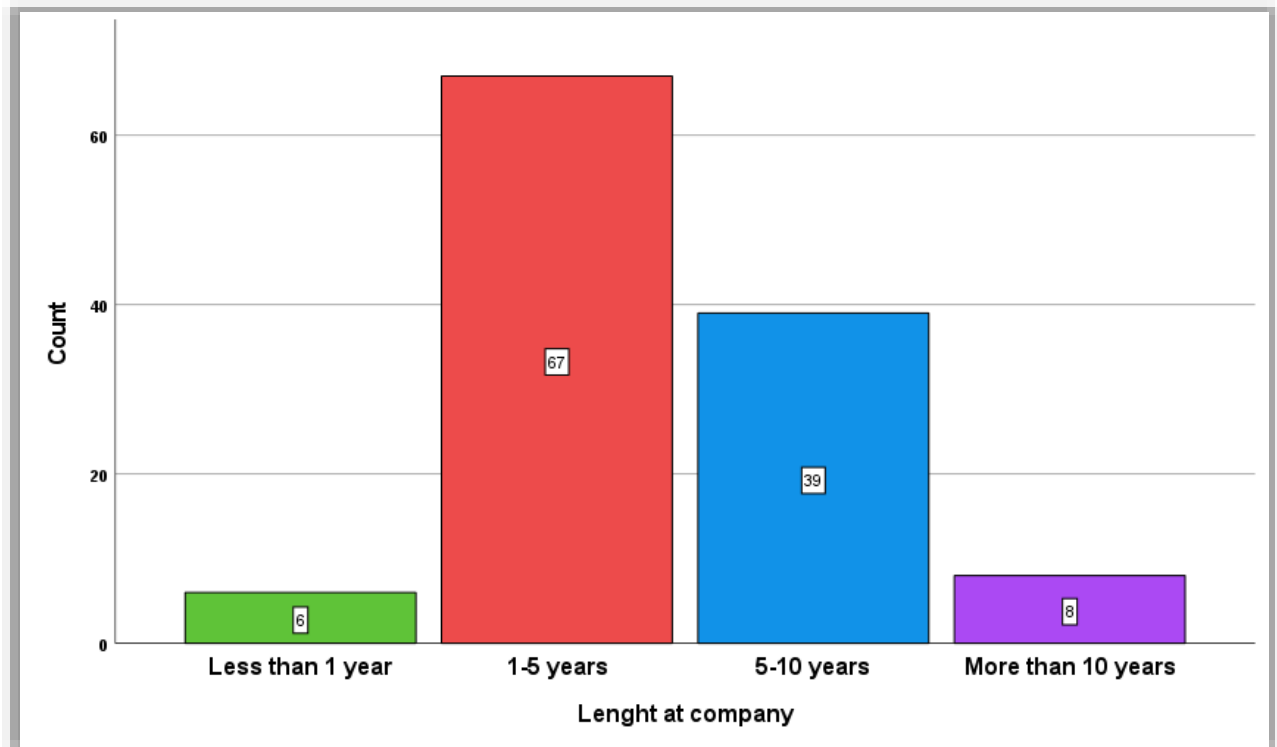


Figure 9: Length at company

4.3.3 Job position

The purpose of this question in the survey was to determine the different job position levels of the respondents at SMEs. According to Figure 10 below, a total of 36 respondents have an executive or owner role, 3 respondents have a senior management role, a total of 29 respondents has a middle management role and 52 of the respondents were employees. This indicates that a majority of the respondents in this study were employees at SMEs.

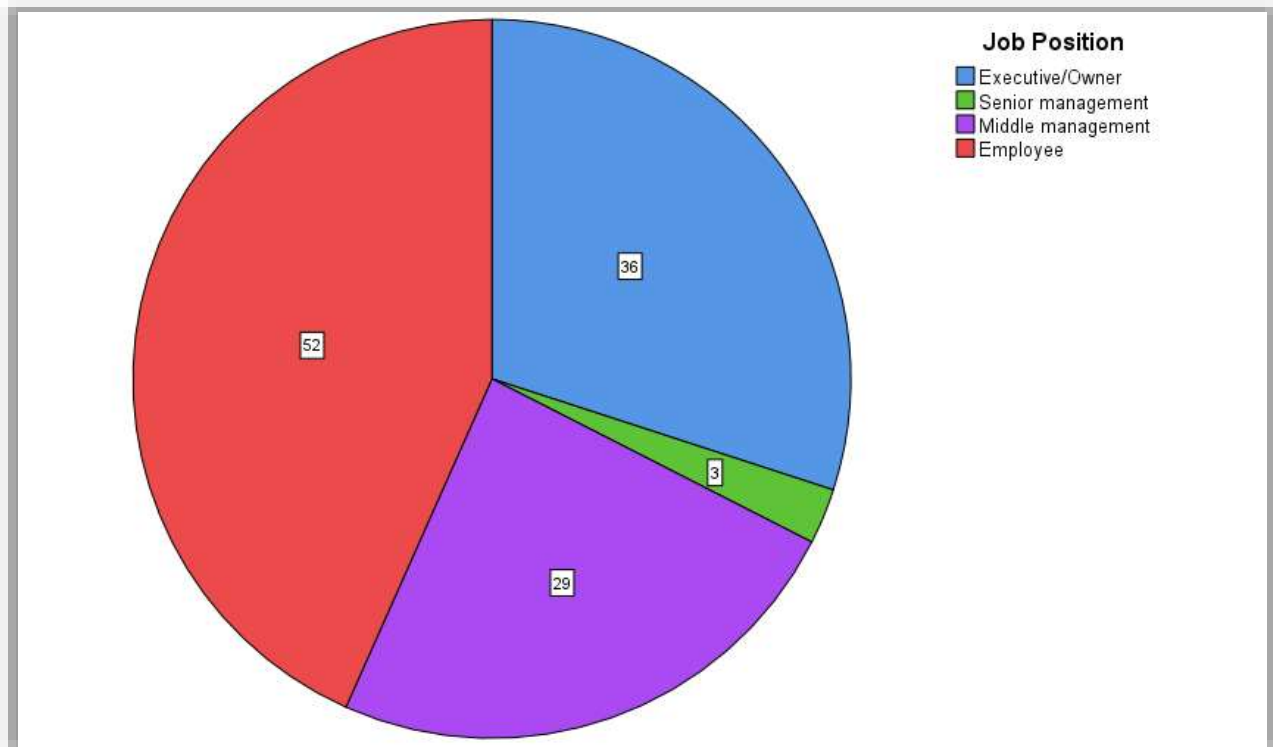


Figure 10: Respondent's job position

4.3.4 Organization type

The purpose of requesting the organization type in the survey was to determine under which type the SMEs in this study fall. The result in Figure 11 below shows that 20 of the respondents fall under retail organizations, 16 respondents fall under technical organizations, 25 respondents work in the health organization, 8 respondents work for personal care businesses, 10 respondents work for law organizations, 38 respondents work in businesses that provide services and 3 respondents work for small businesses that are categorized as other. This is an indication that the majority of respondents in this study work for small businesses that render services to their clients.

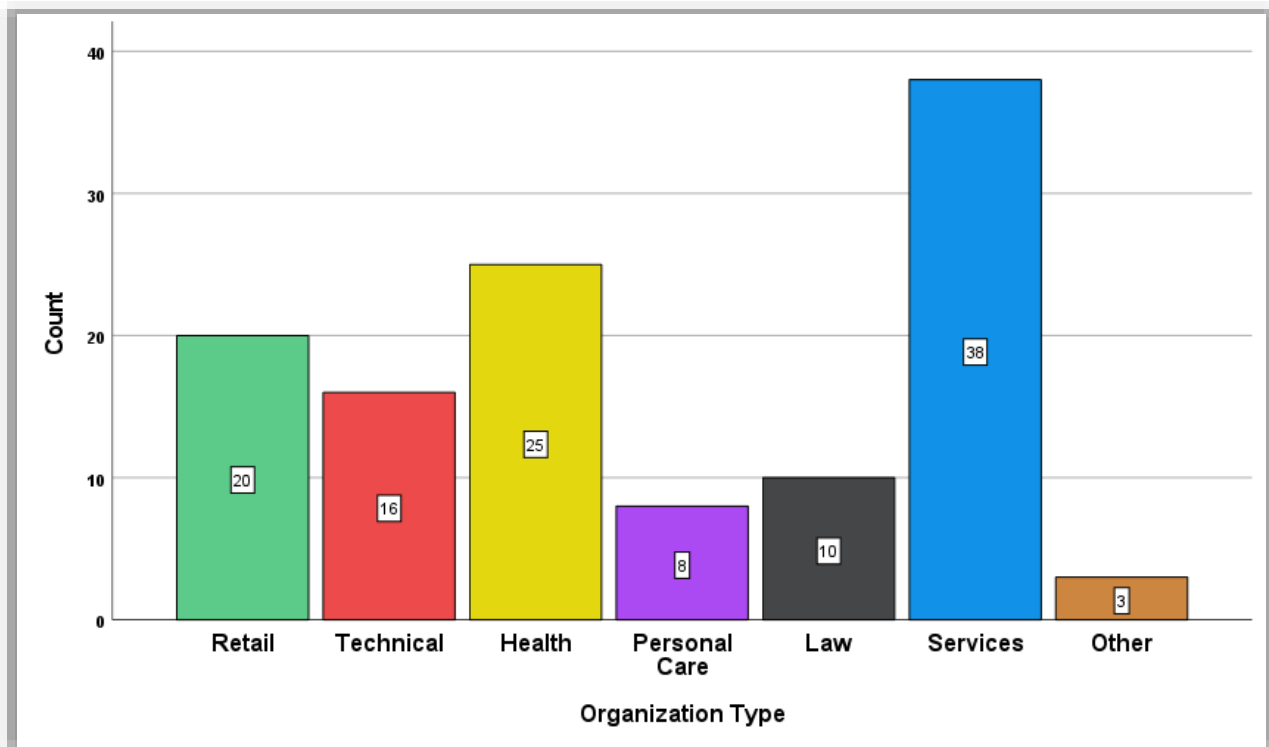


Figure 11: Organization type

4.4 Characteristics of the instrument development

In this section, the researcher will analyze the characteristics of the survey instrument using a Likert scale analysis, reliability through internal consistency, validity through factor analysis, and the normality of the data tested.

4.4.1 Likert scale analysis

According to Joshi, Kale, Chandel, & Pal (2015), “Likert scale is applied as one of the most fundamental and frequently used psychometric tools in educational and social sciences research”. This allows researchers to effectively measure data for analysis purposes. The author further asserts that “the format of a typical five-level Likert item is: 1. Strongly Disagree, 2. Disagree, 3. Neither Agree nor Disagree (undecided or neutral), 4. Agree, 5. Strongly agree”. As shown in Table 9 below, this research study used a five-level Likert item for the survey instrument.

For the researcher to analyze the Likert scale items, in practice all the data and information received from respondents was summarized in the form of mean scores through statistical analysis. The mean scores will therefore be interpreted using an interval length of 0.80 from the lower limit to the upper limit. The interval length for the level of “Strongly agree” has an interval of [1: 1.80] and “Disagree”

has an interval of [1.80: 2.60]. Secondly, the interval length for the level of “Neutral” has an interval of [2.60: 3.40] and the level of “Agree” has an interval of [3.40: 4.20]. Lastly, the interval length at “Strongly agree” has an interval of [4.20: 5]. The mean scores and Likert scale intervals will be used in the next section of the analysis.

Table 9: Likert scale analysis

Level	Scale	Interval length	Lower Limit	Upper Limit	Interval
Strongly Disagree	1	0.80	1	1.80	[1: 1.80)
Disagree	2	0.80	1.80	2.60	[1.80: 2.60)
Neutral	3	0.80	2.60	3.40	[2.60: 3.40)
Agree	4	0.80	3.40	4.20	[3.40: 4.20)
Strongly Agree	5	0.80	4.20	5.00	[4.20: 5]

4.4.2 Reliability (Internal consistency - Cronbach’s alpha)

According to Mohajan (2017), “reliability concerns the faith that one can have in the data obtained from the use of an instrument, that is, the degree to which any measuring tool controls for random error”. The measurement of a research instrument's reliability is whether it consistently produces the same results. Cronbach alpha values were calculated to assess each factor's degree of reliability. Internal consistencies produced by Cronbach's alpha that is more than the minimum value of 0.70 required for acceptable reliability (Cronbach & Shapiro, 1982). However, when using ratio scales, like the Likert scale, a reliability coefficient of 0.58 may be sufficient for analytical scrutiny (Moolla & Bisschoff, 2012).

In Table 10 below, a set of 18 questions were used in the survey for the technological factors and Cronbach’s alpha value was 0.92, which is deemed reliable. There was a set of 24 questions used for the organizational factors and Cronbach’s alpha value was 0.907. This is also deemed reliable. The environmental factors have a set of 18 questions that were used and the Cronbach’s alpha value was 0.907, which is also deemed reliable. This is an indication that all the survey questions used in this study produced internal consistencies higher than 0.90 (exceeding the minimum value of 0.70) which is acceptable for reliability.

Table 10: Reliability statistics of Technological-Organizational-Environmental Factors

Technological Factors - Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.920	.921	18
Organizational Factors - Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.907	.903	24
Environmental Factors - Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.907	.911	18

4.4.3 Validity and factor analysis

Factor analysis and Kaiser-Meyer-Olkin (KMO) sampling adequacy were used to measure the construct validity of the survey questionnaires (Appendix D). The Bartlett test of sphericity was conducted to ensure the factor analysis was appropriate. Below are the factors identified and discussed:

4.4.3.1 Technological factors

The results in Table 11 below present the Kaiser-Meyer-Olkin (KMO) test of sampling adequacy and Bartlett's test of sphericity for section B of the survey questionnaire relating to Technological factors. These factors were tested to examine whether the questions in the survey measure what it is intended to measure. The KMO presented yields a value of **0.853** which is acceptable and higher than the limit of 0.5. When the KMO value falls between 0.8 and 1, it indicates that the sampling in this study is adequate. Consequently, this means that the sample adequately represents the larger population from which it was obtained. The Bartlett's test deemed a value of, $p = < .001$. This is below 0.05, indicating a relatively high correlation. The results in Table 11 reveal that factor analysis can be computed and are presented in Table 12 below.

Table 11: Validity of technological factors

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.853
Bartlett's Test of Sphericity	Approx. Chi-Square	1904.175
	df	153
	Sig.	<.001

The component matrix below (in Table 12) reveals that all the questions relating to the factors named technological complexity, existing technology, and technological compatibility had a factor loading above the limit of 0.3. One valid factor was obtained for the technological complexity (**0.823**) and existing technology (**0.779**) questions and a second valid factor was obtained for the technological compatibility (**0.69**) questions.

Table 12: Component matrix of technological factors

Component Matrix ^a		
	Component	
	1	2
Technological Complexity	.823	
Existing Technology	.779	
Technological Compatibility		.690

4.4.3.2 Organizational factors

The results in Table 13 below present the KMO test of sampling adequacy and Bartlett's test of sphericity for section C of the survey questionnaire relating to Organizational factors. These factors were tested to examine whether the questions in the survey measure what it is intended to measure. The KMO yields a value of **0.873** which is acceptable and higher than the limit of 0.5. Bartlett's test deemed a value of, $p = .000$. Which is below 0.05, indicating a relatively high correlation. The results in Table 13 reveal that factor analysis can be computed and are presented in Table 14 below.

Table 13: Validity of Organizational factors

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.873
Bartlett's Test of Sphericity	Approx. Chi-Square	2958.219
	df	276
	Sig.	.000

The component matrix below (in Table 14) reveals that all the questions relating to the factors named policies and standards, information security awareness, top management support, and organizational learning culture had a factor loading above the limit of 0.3. One valid factor was obtained for the policies and standards (**0.949**) questions and a second valid factor was obtained for the information security awareness (**0.69**), top management support (**0.84**), and organizational learning culture (**0.625**) questions.

Table 14: Component matrix of organizational factors

Component Matrix ^a		
	Component	
	1	2
Policies and Standards	.949	
Information security awareness		.825
Top management support		.804
Organizational learning culture		.625

4.4.3.3 Environmental factors

The results in Table 15 below present the KMO test of sampling adequacy and Bartlett's test of sphericity for section D of the survey questionnaire relating to Environmental factors. These factors were tested to examine whether the questions in the survey measure what it is intended to measure. The KMO yields a value of **0.79** which is acceptable and higher than the limit of 0.5. Bartlett's test deemed a value of, $p = .000$. Which is below 0.05, indicating a relatively high correlation. The results in Table 15 reveal that factor analysis can be computed and are presented in Table 16 below.

Table 15: Validity of Environmental factors

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.790
Bartlett's Test of Sphericity	Approx. Chi-Square	2578.526
	df	153
	Sig.	.000

The component matrix below reveals that all the questions relating to the factors named risks in outsourcing, security regulatory concerns, and security, and privacy compliance had a factor loading above the limit of 0.3. One valid factor was obtained for the risks in outsourcing (**0.791**) and a second valid factor was obtained for the security regulatory concerns (**0.935**) and security and privacy compliance (**0.79**) questions.

Table 16: Component matrix of Environmental factors

Component Matrix ^a		
	Component	
	1	2
Risks in Outsourcing	.791	
Security Regulatory Concerns		.935
Security and privacy Compliance		.790

Therefore, the study found that SMEs' compliance with information security adoption is influenced by the following factors:

- Section B: Technological factors (Technological compatibility, Existing technology, and Technological complexity)
- Section C: Organizational factors (Top management support, Information security awareness, Policies, and standards, Organizational learning culture)
- Section D: Environmental Factors (Risks in outsourcing, Security and Privacy compliance, Security regulatory concerns)

4.4.4 Test for normality

According to Leung (2011), there are three steps to test the normality of Likert scale data: Skewness and kurtosis, Kolmogorov-Smirnov (KS) and Shapiro-Wilk (SW) tests for normality, and lastly normal Q-Q plot. A normality test determines whether data are normally distributed or not. In normal distributions, a significant value is greater than 0.05, whereas, in non-normal distributions, a significant value is less than 0.05. In the case of normally distributed data, parametric tests such as one-way ANOVA, independent samples-test, and Pearson correlation will be used. When the data is not normally distributed, non-parametric tests can be used, such as the Kruskal-Wallis H test, Mann-Whitney U test, or Spearman correlation.

In Table 17 below, the normality test was done using the Kolmogorov-Smirnov and the Shapiro-Wilk test for normality. Leung (2011), describes the KS and SW tests as being used for formal statistical assessment of normality. The author further asserts that the KS test compares a distribution to a reference distribution that is considered normal and the higher the KS statistics, the further it is from a normal distribution. It is also considered less powerful than the parametric SW test, which is used to test normal distributions (different from the KS test), and the higher the SW value, the closer to normality. Both tests use an alpha value of 0.05. Table 17 illustrates that both KS and SW tests yield significance values less than 0.001. This indicates that the data in this study is not normally distributed and will make use of non-parametric tests.

Table 17: Test for normality of data

	Kolmogorov-Smirnova			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Compatibility	.216	120	<.001	.934	120	<.001
Existing Technology	.188	120	<.001	.925	120	<.001
Complexity	.161	120	<.001	.908	120	<.001
Learning Culture	.115	120	<.001	.955	120	<.001
InfoSec Culture	.149	120	<.001	.925	120	<.001
Management Support	.337	120	<.001	.724	120	<.001
Policies & Standards	.267	120	<.001	.801	120	<.001
Security Compliance	.240	120	<.001	.856	120	<.001
Security Regulations	.315	120	<.001	.776	120	<.001

Outsourcing	.174	120	<.001	.916	120	<.001
a. Lilliefors Significance Correction						

4.5 Factors affecting the adoption of information security compliance

This research study used both descriptive statistics and inferential statistics to analyze the collected data. Descriptive statistics can be described as “measures of central tendencies and measures of dispersion” (Cipolla-Ficarra & Ficarra, 2010). Measures of central tendency include the mean, median, mode, frequencies, and percentages. Standard deviations and variance are examples of measures of dispersion. Inferential statistics can be described as “tests that aim to measure the difference, correlation, and association among the different variables” (Osborne, 2010).

According to section 4.5.1, the research instrument was measured on a Likert scale and summarized in terms of mean scores and standard deviation to identify the factors. In the next section, descriptive statistics were used to calculate the mean scores (represented as \bar{X}) and standard deviations (represented as SD). More detailed mean scores and standard deviations are presented in Appendix E. The first three objectives of this research study are to identify the factors that affect SMEs' adoption of information security compliance. For technological, organizational, and environmental factors, mean scores and standard deviations are shown below.

4.5.1 Technological factors

To interpret the technological factors identified in this study, mean scores and standard deviations were computed in Table 18 for section B of the survey questionnaire. The first factor is identified as the “existing technology” in organizations and has a mean score of 3.98 and 0.79 standard deviations. As a result, the majority of respondents believe their technological skills and experience impact their compliance with information security policies. The second highest mean score is the factor identified as “technological compatibility”. This factor has a mean score of 3.37 and a standard deviation of 0.89. The results indicate that respondents agree that internal information systems applications affect information security compliance. The last factor is “technological complexity” which has the lowest mean score of 2.95 and a standard deviation of 1.03. This indicates that some employees have a neutral view that the inherent quality of information technology (IT) influences information security compliance in the workplace.

Table 18: Technological factors

Descriptive statistics	N	Minimum	Maximum	\bar{X}	SD
Technological Compatibility	120	1	5	3.3736	.89333
Existing Technology	120	1	5	3.9819	.79533
Technological Complexity	120	1	5	2.9542	1.03083
Valid N (listwise)	120				

4.5.1.1 Correlation

In this study, non-normal distributed data will be analyzed using non-parametric tests. Spearman's rho correlation matrix was used to show the correlation coefficients between the identified technological factors. It will establish whether there is a positive or negative correlation between the factors based on the two asterisks next to it as highlighted in Table 19 below.

Table 19: Correlation matrix of the technological factors

Spearman's rho		Compatibility	Technology	Complexity
Compatibility	Correlation Coefficient	1.000	.541**	.459**
	Sig. (2-tailed)	.	.001	.001
Technology	Correlation Coefficient	.541**	1.000	.510**
	Sig. (2-tailed)	.001	.	.001
Complexity	Correlation Coefficient	.459**	.510**	1.000
	Sig. (2-tailed)	.001	.001	.

** . Correlation is significant at the 0.01 level (2-tailed).

The results in Table 19 indicate that there was a highly statistically significant positive correlation between the two factors identified as technological compatibility and existing technology, $r(120) = .541^{**}$, $p = .001$. This reveals that the SMEs current security technology fits well with the existing technology setting in the company. There is also a medium statistically positive correlation between the two factors technological compatibility and technological complexity, $r(120) = .459^{**}$, $p = .001$. This is an indication that the current quality of the security technology has a positive impact on the employees' ability to adapt to the inherent quality of the company's IT system. A similar high statistically significant positive correlation was found between the factors identified as existing technology and technological complexity, $r(120) = .510^{**}$, $p = .001$. This result reveals that the

existing technology in the company fits well with the employee’s ability to keep up with the constant change and upgrade of the company’s IT system. To conclude, the results suggest a high positive correlation between technological factors.

4.5.2 Organizational factors

For section C of the survey questionnaire, mean scores and standard deviation were calculated in Table 20 to interpret the organizational factors identified. The first organizational factor is identified as the “organizational learning culture”. This factor has a mean score of 3.32 and a standard deviation of 0.86. Accordingly, the majority of the respondents agree that learning characteristics and organizational orientation affect information security compliance. The second factor is identified as “policies and standards” and has a mean score of 3.23 with a standard deviation of 0.98. Based on the results, most respondents believe guidelines, procedures, and technical controls specified in InfoSec policies have an impact on information security.

The third factor is identified as the “information security culture”. This factor has a mean score of 3.00 and a standard deviation of 0.96. Based on this, respondents also have a neutral view that the value of complying with information security standards and policies has an impact on information security compliance. The last factor is “top management support” which has a mean score of 2.18 and a standard deviation of 0.54. This indicates that the majority of respondents disagree that senior management promotes information security. Therefore, no support from senior management has an impact on the employee’s compliance

Table 20: Organizational factors

Descriptive statistics	N	Minimum	Maximum	\bar{X}	SD
Learning Culture	120	1	5	3.3222	.8665
Policies and standards	120	1	5	3.2361	.98033
InfoSec Culture	120	1	5	3.0014	.96283
Management Support	120	1	5	2.1819	.54366
Valid N (listwise)	120				

4.5.2.1 Correlation

As discussed in section 4.5.4 above, non-normal distributed data will be used and analyzed using non-parametric tests. Spearman's rho correlation matrix was also used to show the correlation coefficients

between the identified organizational factors. The positive and negative correlation between the factors is highlighted in Table 21 below.

Table 21: Correlation matrix of organizational factors

Spearman's rho		Learning Culture	InfoSec awareness	Management Support	Policies & Standards
Learning Culture	Correlation Coefficient	1.000	.673**	.203*	.669**
	Sig. (2-tailed)	.	.001	.026	.001
InfoSec Awareness	Correlation Coefficient	.673**	1.000	.459**	.551**
	Sig. (2-tailed)	.001	.	.001	.001
Policies & standards	Correlation Coefficient	.669**	.551**	.285**	1.000
	Sig. (2-tailed)	.001	.001	.002	.
Management Support	Correlation Coefficient	.203*	.459**	1.000	.285**
	Sig. (2-tailed)	.026	.001	.	.002

** . Correlation is significant at the 0.01 level (2-tailed).

* . Correlation is significant at the 0.05 level (2-tailed).

There was a high statistically significant positive correlation between the factors called organizational learning culture and Information security awareness, $r(120) = .673^{**}$, $p = .001$. This shows that the company's ability to learn new technology has a positive impact on the way employees perceive information security in the workplace. Also, there is a small statically significant positive correlation between the factors of organizational learning culture and top management support, $r(120) = .203^*$, $p = .026$. This reveals that the support from top management to employees does not guarantee that the company will be able to successfully adapt to new technology. There is a highly statistically significant positive correlation between the factors identified as organizational learning culture and policies and standards, $r(120) = .669^{**}$, $p = .001$. This indicates that the employee's ability to adapt to new technology or innovation causes them to focus more on being compliant with the company's security policies and standards.

There was a medium statistically significant positive correlation between the factors of information security awareness and top management support, $r(120) = .459^{**}$, $p = .001$. The support received

from top management creates employees to value the security policies and standards in the company by being more compliant. Also, there is a highly statistically significant positive correlation between the factors of information security awareness and policies and standards, $r(120) = .551^{**}$, $p = .001$. This shows that the more employees are aware of the security culture in their workplace, the more they will feel the need to be compliant with the security policies and standards. Lastly, there is a small statistically significant positive correlation between policies and standards and top management support, $r(120) = .285^{**}$, $p = .002$. This reveals that the support received from top management does not guarantee compliance of employees with the company's security policies and standards. The correlation matrix shows a high to a small positive correlation between the organizational factors based on the results presented.

4.5.3 Environmental factors

To interpret the environmental factors identified in this study, mean scores and standard deviations for section D were calculated. The first environmental factor identified in Table 22 below is the “security and privacy compliance” factor which has a mean score of 3.82 and a standard deviation of 0.70. According to the majority of respondents, they agree that they are compliant with the information security policies and standards that are set out by the organization. The second factor is the “security regulations”. This factor has a mean score of 2.65 and a standard deviation of 1.00. This indicates that a majority of respondents have a neutral view that the organizational concerns in ensuring compliance with security and data privacy regulations have an impact on their information security compliance. The last factor is identified as the “risk of outsourcing”. This factor has a mean score of 2.73 and a standard deviation of 0.90. Based on this result, the respondents have a neutral view of the associated security and privacy risks that may result from an organizational decision to outsource their data protection to enforce information security compliance.

Table 22: Environmental factors

Descriptive statistics	N	Minimum	Maximum	\bar{X}	SD
Security Compliance	120	1	5	3.8236	.7055
Security regulations	120	1	5	2.6583	1.00783
Risk of outsourcing	120	1	5	2.7306	.90117
Valid N (listwise)	120				

4.5.3.1 Correlation

Spearman’s rho non-parametric test was used to analyze the data collected for section B of the questionnaire that covered the environmental factors. In Table 23 below all the environmental factors are identified to interpret the positive and negative correlation coefficients between the factors.

Table 23: Correlation matrix of organizational factors

Spearman’s rho		Security Compliance	Security Regulations	Outsourcing
Security Compliance	Correlation Coefficient	1.000	.022	.463**
	Sig. (2-tailed)	.	.812	.001
Security regulations	Correlation Coefficient	.022	1.000	.149
	Sig. (2-tailed)	.812	.	.104
Outsourcing	Correlation Coefficient	.463**	.149	1.000
	Sig. (2-tailed)	.001	.104	.

** . Correlation is significant at the 0.01 level (2-tailed).

According to the results presented in Table 23, there was a very small statistically significant positive correlation between the factors called security compliance and security regulations, $r(120) = .022$, $p = .812$. This reveals that the company’s ability to be compliant with the information security adoption does guarantee that there will be value in complying with the security regulations from employees. However, there was a medium statistically significant positive correlation between the security compliance factor and the risk of outsourcing factor, $r(120) = .463^{**}$, $p = .001$. This indicates that if the company decides to outsource its information security and accept the risks, there is no guarantee that the company will be compliant with the information security policies and standards. Lastly, there was a very small positive correlation between the factors identified as security regulations and the risk of outsourcing, $r(120) = .149$, $p = .104$. This shows that if the company outsources its information security, there is little to no guarantee that the company will be compliant with the information security regulations. According to this result, the environmental factors identified in this study have a small to medium positive correlation.

4.6 The relationship between the T-O-E factors

Due to the lack of outliers and non-normal distribution of data, the non-parametric Spearman's rho correlation was used. The Spearman's rho correlation matrix has coefficients that fall between -1 and 1, with -1 denoting a fully negative correlation between two variables, 0 denoting no correlation between two variables, and 1 denoting a perfectly positive correlation between two variables (Kothari, 2004). Table 24 presents the factors that have two asterisks (**) that indicate a large to a medium positive correlation between the two factors and that the data presented are statistically significant. Whereas the sections that have no asterisks indicate there is no statically significant correlation. However, where there is one asterisk (*) present, it is an indication that there is a small to medium positive correlation. Also, there is a small correlation when the value is 0.1, a medium correlation when the value is 0.3, and a large correlation when the value is 0.5 and higher.

Table 24: Correlation matrix

Spearman's Rho		Learning Culture	InfoSec awareness	Management Support	Policies Standards	Security Compliance	Security Regulations	Outsourcing
Compatibility	Coefficient	.559**	.639**	.338**	.653**	.395**	.007	.418**
	Sig. (2-tailed)	.001	.001	.001	.001	.001	.939	.001
Technology	Coefficient	.491**	.635**	.368**	.504**	.342**	-.013	.407**
	Sig. (2-tailed)	.001	.001	.001	.001	.001	.884	.001
Complexity	Coefficient	.592**	.773**	.366**	.422**	.282**	-.065	.361**
	Sig. (2-tailed)	.001	.001	.001	.001	.002	.479	.001
		Compatibility	Technology	Complexity	Learning Culture	InfoSec awareness	Management Support	Policies Standards
Security Compliance	Coefficient	.395**	.342**	.282**	.390**	.384**	.411**	.593**
	Sig. (2-tailed)	.001	.001	.002	.001	.001	.001	.001
Security Regulations	Coefficient	.007	-.013	-.065	-.107	-.016	.228*	-.095
	Sig. (2-tailed)	.939	.884	.479	.245	.863	.012	.302
Outsourcing	Coefficient	.418**	.407**	.361**	.327**	.495**	.466**	.481**
	Sig. (2-tailed)	.001	.001	.001	.001	.001	.001	.001

All highlighted sections indicate a high to medium correlation and will be explained below.

This study reveals that there was a high statistically significant correlation between the two factors called technological compatibility and organizational learning culture, $r(120) = .559^{**}$, $p = .001$. This shows that SMEs that can easily adapt to new technology have strong technological compatibility that fits with the needs and values of their organizations. There was a high statistically significant correlation between the factors of technological compatibility and information security awareness, $r(120) = .639^{**}$, $p = .001$. Employees who value information security compliance can adapt to new technology without violating any security policies or standards. The results show that there was a medium statistically significant correlation between the factors of technological compatibility and top management support, $r(120) = .338^{**}$, $p = .001$. Accordingly, top management commitment and support promote the fit between new technology and adopters' values and needs.

There was a high statistically significant correlation between technological compatibility and security policies and standards, $r(120) = .653^{**}$, $p = .001$. Employees are easily able to adapt to new technologies because SMEs implement information security rules and guidelines. The study reveals that there was a medium statistically significant correlation between the two factors called technological compatibility and security compliance, $r(120) = .395^{**}$, $p = .001$. Therefore, SMEs that monitor and assess their employees based on their compliance with information security adoption do not guarantee that it affects their needs and values. Also, there was a medium statistically significant correlation between the factors named technological compatibility and the risk of outsourcing, $r(120) = .418^{**}$, $p = .001$. SMEs that outsource their security are more likely to have employees who are comfortable adapting to new technology.

According to this study, there was a medium statistically significant correlation between the two factors called existing technology and organizational learning culture, $r(120) = .491^{**}$, $p = .001$. The ability of SMEs to adapt to innovations using their existing technology sets the tone for how they approach complicated technologies. There was a high statistically significant correlation between the factors of existing technology and information security awareness, $r(120) = .635^{**}$, $p = .001$. Therefore, management's approach to promoting information security in the workplace will enable employees to use existing technology efficiently. The results show that there was a medium statistically significant correlation between the factors of existing technology and top management support, $r(120) = .368^{**}$, $p = .001$. As a result, it becomes clear that how much technology adoption can be achieved by the organization depends on the commitment and support of top management.

There was a high statistically significant correlation between existing technology and security policies and standards, $r(120) = .504^{**}$, $p = .001$. This correlation reveals that how SMEs protect and manage their resources affects the existing technology of the organization. The study reveals that there was a medium statistically significant correlation between the two factors called existing technology and security compliance, $r(120) = .342^{**}$, $p = .001$. This indicates that the SMEs existing technology fits well with the way employees comply with the security policies and standards. Also, there was a medium statistically significant correlation between the factors named existing technology and the risk of outsourcing, $r(120) = .407^{**}$, $p = .001$. This shows that the organization's existing technology will allow the organization ability to take the risk of outsourcing.

The results of this study reveal that there was a high statistically significant correlation between the two factors called technological complexity and organizational learning culture, $r(120) = .592^{**}$, $p = .001$. SMEs with strong learning capabilities will be able to adapt to new technology regardless of the quality of their IT system. There was a high statistically significant correlation between the factors of technological complexity and information security awareness, $r(120) = .773^{**}$, $p = .001$. It suggests that employees' belief in the value of compliance with information security policies and standards is affected by the uncertainty surrounding technology in SMEs. The results show that there was a medium statistically significant correlation between the factors of technological complexity and top management support, $r(120) = .366^{**}$, $p = .001$. As a result, the quality and complexity of technology in SMEs are associated with the level of commitment and support from top management in the company.

There was a medium statistically significant correlation between technological complexity and security policies and standards, $r(120) = .422^{**}$, $p = .001$. As a result of the constant upgrades and changes to complex technology in SMEs, management is stricter about setting rules and guidelines for information security policies and standards to ensure that assets and resources are utilized correctly. Also, there was a medium statistically significant correlation between the factors named technological complexity and the risk of outsourcing, $r(120) = .361^{**}$, $p = .001$. As a result of the complexity of technology, SMEs are considering outsourcing their security and accepting the risks that come with that. There was a medium statistically significant correlation between the two factors called security compliance and organizational learning culture, $r(120) = .390^{**}$, $p = .001$. According to this result, the learning culture and the ability of SMEs to adapt to new technology are important factors that influence how they monitor and assess systems to ensure they comply with regulatory requirements.

There was a medium statistically significant correlation between the factors of security compliance and information security awareness, $r(120) = .384^{**}$, $p = .001$. It appears that the more employees are aware of the company's information security policies and standards, the more likely they are to comply with how they use and assess the systems at work. The results show that there was a medium statistically significant correlation between the factors of security compliance and top management support, $r(120) = .411^{**}$, $p = .001$. Accordingly, how employees use the IT and security systems at work is influenced by the support from top management. There was a high statistically significant correlation between security compliance and security policies and standards, $r(120) = .593^{**}$, $p = .001$. As a result, it indicates how effectively employees comply with regulatory requirements in terms of understanding and valuing information security policies and standards.

The results in Table 24 show that there was a medium statistically significant correlation between the two factors called risk of outsourcing and organizational learning culture, $r(120) = .327^{**}$, $p = .001$. SME learning cultures and adaptability to new technologies will be affected if they outsource their security and accept the risks. There was a medium statistically significant correlation between the factors of risk of outsourcing and information security awareness, $r(120) = .495^{**}$, $p = .001$. In SMEs, outsourcing security systems affects information security awareness among employees. The results show that there was a medium statistically significant correlation between the factors of the risk of outsourcing and top management support, $r(120) = .466^{**}$, $p = .001$. This reveals that the tools and services provided by outsourcing professionals encourage top management support and commitment to employees. There was a medium statistically significant correlation between the risk of outsourcing and security policies and standards, $r(120) = .481^{**}$, $p = .001$. This shows that when SMEs decide to outsource their security it will have a positive impact on their security policies and standards.

4.7 The relationship between job position and experience

As the data in this study are not normally distributed, the Kruskal-Wallis H test is used to determine the relationship between job position and experience and information security compliance. According to Ostertagova, Ostertag, & Kováč (2014), the Kruskal-Wallis H test can be described as a rank-based test and is considered useful in the comparison of two and more independent samples. The authors further assert that “the test is a powerful alternative to the One-way analysis of variance and it tests whether samples come from the same distribution”. If the Kruskal-Wallis test is significant, nonparametric multiple comparison tests may be used to further analyze the data (Pohlert, 2014).

Table 25: Relationship between job position and experience

Test Statistics ^{a,b}	
	Compliance
Kruskal-Wallis H (Chi-square)	4.926
Df	3
Asymp. Sig.	.177

a. Kruskal Wallis Test

b. Grouping Variable: Job experience

The results of the Kruskal-Wallis H Test reveal that there is no statistically significant difference between the three groups named job position, experience, and security compliance, $H(3) = 4.926$, $p = 0.177$. This indicates that management and employees' experience in their job position does not guarantee that they will comply with the information security policies and standards in the workplace to meet the regulatory requirements.

4.8 The successful adoption of InfoSec compliance

A regression analysis was conducted to examine whether an effective information security policy predicts the successful adoption of information security compliance. Regression analysis “allows market researchers to analyze relationships between one independent and one dependent variable” (Sarstedt & Mooi, 2014). Before conducting the regression analysis, the dependent variable (information security compliance) and independent variable (information security policy) were tested for normality and presented in section 4.9.1 below.

4.8.1 Normality test

A scatter plot was computed to present the relationship between information security policies influences the successful adoption of information security compliance. In Figure 12 below, the relationship between the two factors is positive and linear with no bivariate outliers. Based on the standard residuals, there were no outliers in the data (Std. Residual Min. = -3.449, Std. Residual Max. = 2.437). A Durbin-Watson test was used to confirm residual error independence ($d = 1.534$). It was evident from residual plots that the residuals were homoscedastic and normal. The regression equation for predicting the successful adoption of Information security compliance from policies and standards in SMEs was $\hat{y} = 2.86 + 0.3*x$.

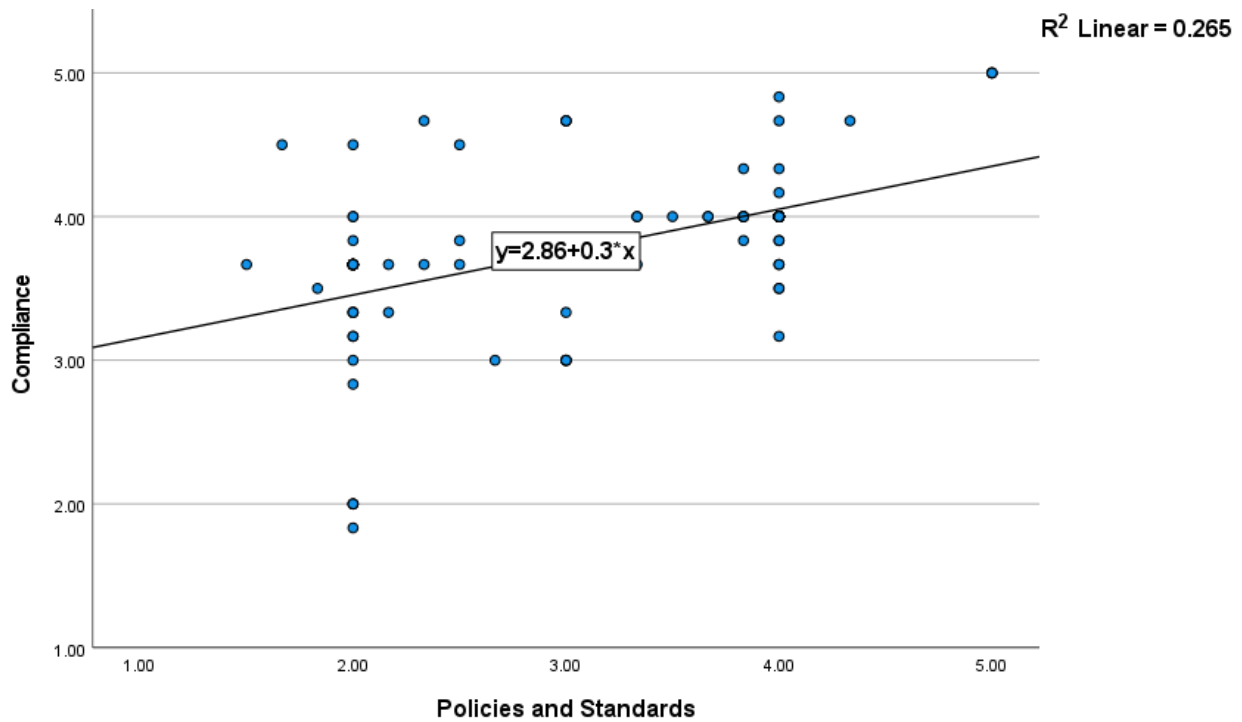


Figure 12: Scatterplot of data

4.8.2 Simple linear regression

As revealed in the table of regression (Table 26), the value of the correlation coefficient is $R = .515$ (51.5%). This indicates that there was a positive link between policies and standards set by SMEs regarding information security which led to the successful adoption of information security compliance. However, only 26.5% (R Square value = **.265**) was accounted for in the information security policies and standards. The adjusted R Square has a value of 25.9% (Adj. R = **.259**) which indicates that the six factors of policies and standards will account for more than 25.9% of the factors that influence the successful adoption of InfoSec compliance. The standard error of the estimates has a value of (Std. error = **.47002**) which represents the standard deviation of the observed scores presented around the regression line. The change statistics in Table 26 have a value of $F(1,118) = 42.516$, $p = .001$. This indicates that the F-statistics created ($F = 42.516$) were significant at a 1 percent level (Sig. f = **<0.001**) with the value of 1 to 118 degrees of freedom, therefore the fitness for the model is approved.

Table 26: Regression model summary

Model Summary										
Model	R	R Square	Adj. R Square	Std. error	R Square Change	F Change	df1	df2	Sig. F Change	Durbin-Watson
1	.515	.265	.259	.47002	.265	42.516	1	118	<.001	1.534

- a. Predictors: (Constant), Policies and Standards
- b. Dependent Variable: Compliance

The analysis of variance presented in Table 27 below, indicates that the policies and standards have a statistically significant prediction of the successful adoption of information security compliance in SMEs, $F(1,118) = 42.516$, $p < .001$. This indicates that the F-statistics created ($F = 42.516$) were significant at a 1 percent level ($\text{Sig. } f = <0.001$) with the value of 1 to 118 degrees of freedom, therefore the fitness for the model is approved.

Table 27: Analysis of variance

ANOVA ^a						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	9.393	1	9.393	42.516	<.001 ^b
	Residual	26.068	118	.221		
	Total	35.461	119			

- a. Dependent Variable: Compliance
- b. Predictors: (Constant), Policies and Standards

The results in Table 28 below present the impact of policies and standards on the successful adoption of information security compliance in SMEs. The results revealed that there is a positive statistically significant impact on the successful adoption of InfoSec compliance. Policies and standards predict an impact on compliance behaviour revealed as, ($B1 = .299$). Considering the results this study can successfully say that the effective use of policies and standards in SMEs leads to the successful adoption of information security compliance.

Table 28: Regression Coefficients

Coefficients ^a						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.857	.154		18.510	<.001
	Policies & Standards	.299	.046	.515	6.520	<.001

a. Dependent Variable: Compliance

4.9 Practical recommendations for SMEs

The purpose of this section is to make practical recommendations to SMEs regarding the factors that affect information security compliance based on the results of the study. Among the ten factors that affect information security adoption, the study makes the following recommendations:

4.9.1 Technological compatibility

It is recommended that SMEs make sure that the technology and innovation in the workplace fit well with the employee’s skills, values, and previous practices. Management can provide additional training to employees if the quality of the IT systems is not compatible with their skills and current needs. This will encourage employees to make sure that the IT systems work well together without any challenges of altering the quality of the technology.

4.9.2 Technological complexity

It is recommended that the management in SMEs implement policies that motivate employees to speak up about the use of complex technology in the workplace. The use of different social support programs can also be implemented to ease the use of complex technology. Employees should feel comfortable reaching out for assistance when faced with technological challenges to encourage self-efficacy.

4.9.3 Existing technology

It is recommended that the existing technology setting in SMEs always fit with the intended technology innovation that the organization wishes to adopt. It is important for SMEs to always search

for strengths and gaps in their technology systems before undertaking new technology innovations. This can be done through meeting with experts that will analyze the existing technology to determine how much technology adoption the organization can take.

4.9.4 Organizational learning culture

It is recommended that SMEs invest in learning capabilities so that they can learn new technology, identify opportunities, provide practical solutions, and have processes in place to scan for risks. This can be done by implementing the use of e-Learning to meet the needs of the organization. This can be achieved through management practices that can encourage employees to use eLearning solutions to acquire new skills, knowledge, and competencies.

4.9.5 Information security awareness

It is recommended that SMEs get their management involved in engaging with employees to make sure they understand how crucial information security is in the workplace. Management's involvement will ensure that employees know what their responsibilities are and that information security is a high priority. Practices like investing in security training through internal or external training and making it mandatory for all employees. Free online training is recommended for small and medium organizations.

4.9.6 Top management support

It is recommended that SMEs always stay updated on what their employee's needs and challenges are in the workplace. To encourage information security compliance it is recommended that management provide effective training to employees that might find it challenging to be compliant with the policies and standards of the organization. Regular surveys can be circulated in the workplace so that management can get a sense of what the challenges are and how to overcome them. This will also provide management with information on what training to offer to employees.

4.9.7 Policies and standards

It is recommended that SMEs make sure that their security policies and standards are strong enough to cover the business and its customers. Management and employees should always be aware of the penalties that involve violations of security and privacy. The organization can practice compliance through annual security audits that examine any changes to the current security policies and standards.

In addition, security audits can also determine SMEs whether policies and standards should be updated.

4.9.8 Security and privacy compliance

It is recommended that SMEs invest in appointing a legal compliance officer to make sure that the organization is compliant with security laws and regulations. This can be a full or part-time role in the organization to oversee the day-to-day operations that involve confidential data and information. The option of completely outsourcing their security to companies that specializes in security and privacy compliance is also available to a small business that can afford it.

4.9.9 Privacy and security regulations

It is recommended that SMEs stay updated on any changes in the law and regulations of information security like the POPI Act. Top management can work together with the legal compliance officer (recommended in section 4.10.8) to stay updated on any changes and how they will affect the organization's operations. A top-down approach will be useful in this regard where top management understands the changes and implications of new laws and regulations before they inform employees.

4.9.10 Risks in outsourcing

It is recommended that SMEs consider investing in outsourcing their security to a professional and highly recommended security company. This will enable the organization to deal with security professionals that provide solutions and opportunities that benefit the organization's information security policies, standards, and compliance. The benefits of outsourcing an organization's information security can also be considered when deciding if it is a great fit for the company. The risks in outsourcing should also be considered as to how to overcome these risks. The following benefits, risks, and steps to manage the risks are discussed below.

Benefits of outsourcing include:

- The outsourcing company provides 24/7 coverage throughout the year
- Providing reliable and sustainable systems
- A proactive approach to detecting and responding to threats
- Security standards will be well-documented
- An in-depth understanding of regulatory requirements

Risks in outsourcing:

- Look out for any hidden costs in your contract.
- Be aware and prepared for biased decisions regarding software
- There will be the risk of dependence barriers.
- Be aware of the outsourcing firm will have access to the organization's information systems
- The organization might incur legal consequences if compliance regulations are not met.

Steps to manage outsourcing risks:

- Establish Service Level Agreements (SLAs) with clear definitions of the outsourcing scope, roles and responsibilities, tasks, and timelines.
- As part of the agreements, key issues related to staff management should be addressed like monitoring access to the workplace.
- To ensure security is properly tested, request approval from the oversight team before deploying any systems and tools.
- All internal and service provider staff should be subjected to social engineering tests and mock incidents to ensure they respond appropriately.
- To ensure the service provider reports all findings, build known vulnerabilities into applications before beginning penetration testing.

4.10 Chapter Summary

The chapter starts by introducing the chapter in **Section 4.1. Section 4.2:** An overview of the survey responses is presented with a return rate of 60%. **Section 4.3:** The biographic information of the respondents is given with half of the respondents being female and the other half being male. The length of the company, the job positions, and the organization types are also discussed in section 3. **Section 4.4:** Characteristics of the instrument development were discussed by examining the questions of the survey questionnaire using Likert scale analysis. Also, the reliability of the questions was tested using Cronbach's alpha at internal consistency. The validity and factor analysis were also computed using the Kaiser-Meyer-Olkin and Barlett test of sphericity. Lastly, the data were tested for normality and came back as non-normal distributed data. **Section 4.5:** In this section, the study examined the results of the analysis using mean scores and a correlation matrix for the technological, organizational, and environmental factors. **Section 4.6:** This section discussed result 4 which related to the correlation matrix between the TOE factors to see if there was a relationship between the

factors. **Section 4.7:** This section examined the relationship between job position and job experience to indicate whether the two factors demonstrate successful information security compliance in the workplace. **Section 4.8:** Examined whether an effective information security policy predicts the successful adoption of information security compliance using a normality test with a scatterplot figure and a simple linear regression analysis. **Section 4.9:** Lastly, the study provided practical recommendations to SMEs drawn from the results of the study. The following chapter is called the conclusion of the study where the research problem and research objectives will be revisited.

Chapter 5: Conclusion & Recommendation

5.1 Introduction

In the previous chapter called the results, the researcher presented the data analysis derived from the data collection through descriptive and inferential statistics. This chapter will conclude the study by giving an overview of the previous chapters as well as the results from the analysis of this study. Crossley (2021), describes the conclusions chapter as “the final major chapter of a study that serves as a concluding summary of your research findings”.

The chapter begins by giving an overview of the research questions and sub-questions of the study. Then, the study will re-examine the research aims and objectives to indicate how the results of this study fit with the research aims and objectives. Also, a summary of chapters 1, 2 & 3 is provided with an overview of the results of this study. Then, a critical evaluation is done of the research objectives, and recommendations are given for the study. Lastly, the limitations of the study are discussed with suggestions for future studies.

5.2 Main research question and sub-questions

The main research question in this study was:

Main research question:

What are the factors affecting the adoption of information security compliance among SMEs?

The research sub-questions were:

1. What technological factors are impacting SMEs' adoption of information security compliance?
2. What organizational factors are influencing SMEs' adoption of information security compliance?
3. What environmental factors affect the adoption of information security compliance by SMEs?
4. What recommendations can be made to assist SMEs in meeting their information security compliance obligations?

5.3 Re-examine the aims and objectives of the study

The purpose of the last chapter was to re-examine the research aims and research objectives to determine if they were achieved during the study. The research aim was to assess the importance of information security in small and medium enterprises by identifying the factors that contribute to information security adoption challenges. The results of this study aim to contribute towards improved security management systems for small to medium businesses as well as greater accountability, integrity, and governance among employees. The objectives of this study were:

- To determine the technological factors affecting the adoption of information security compliance among SMEs.
- To determine the organizational factors affecting the adoption of information security compliance among SMEs.
- To determine the environmental factors affecting the adoption of information security compliance among SMEs.
- To make recommendations on ways to improve the adoption of information security compliance among SMEs.

5.4 Summary of the research study

Throughout the current study, the researcher provides summaries of each chapter with an emphasis on the study's objectives.

5.4.1 Chapter 1

Chapter 1 provided the background and nature of this study. In the chapter, the researcher identified a problem in SMEs: SMEs hold sensitive data about their employees, customers, and business partners, they tend to have limited resources to acquire and implement security mechanisms in their organizations and do not have a dedicated IT management department that can handle these responsibilities (Sulayman, Urquhart, Mendes, & Seide, 2012; Leung, 2012). As the importance of information security has grown, organizations have been under pressure to comply with information security policies and standards regarding the protection of company data (AlKalbani, Deng, Kam, & Zhang, 2017). The study used the following points to study the factors of information security adoption.

According to Kent, Tanner, & Kabanda (2016), SME insights regarding information security are difficult to predict mainly because of three reasons:

- SMEs prefer to focus on regulatory compliance rather than protecting their organization's security.
- Restricted resources had a negative attitude toward security because there seems to be no immediate return on investment.
- The belief is that SMEs, particularly start-ups, will not become a target for security attacks.

Therefore, it is important to study the factors that influence information security adoption in SMEs by identifying what factors are preventing SMEs from adopting information security in their organization by determining the factors from a technological, organizational, and environmental perspective.

5.4.2 Chapter 2

Chapter 2 presented the literature review of the study by reviewing all the relevant concepts of the study from a broader context and filtering it down to the level of the study. The chapter starts by discussing the term Small-medium enterprises. An overview of SMEs is presented with various definitions in the context of South Africa, the role of SMEs in South Africa was also discussed, and lastly the challenges of SMEs as a business. In the next section, the literature review conceptualizes the term Information through definition. The importance of information was discussed. After discussing what an SME is and defining information, the literature review discusses Information security (InfoSec). The aspects that were covered included defining information security, information security principles, information security policies (ISP), information security standards, information security controls, and compliance. In the following section, the topic of information security governance was discussed by looking at King IV, the Electronic Communications and Transactions Act (ECT), and lastly the Protection of Personal Information Act (POPIA). Then, the last section of the literature review discussed the information security theories and frameworks. An in-depth discussion was provided of the Institutional theory as well as the Technological-Organizational-Environmental Framework (TOE). Then, the chapter concludes with a chapter summary.

5.4.3 Chapter 3

Chapter 3 presented the research methodology and design of the study using the research onion developed by Saunders, Lewis, and Thornhill (2019). The research onion covered the research

philosophy, approach to theory development, methodological choice, research strategies, the time horizon of the study, as well as the techniques and procedures. The chapter explored the research philosophies and discovered that the study falls in line with the positivism research paradigm. Then, the chapter explored and discussed the research approach and chose a deductive research approach for this study. The methodological choices were also discussed and the quantitative research design was used to gather data for this study. All research strategies were discovered and the strategy for this study was the survey strategy. The research time horizon was also important to outline the timeframe of the study that focussed on a cross-sectional time horizon. Lastly, the chapter presented the techniques and procedures for data collection and analysis. The data collection included the simple-random sampling technique, primary data collection, instrument development, the validity and reliability of the survey questionnaire, and the disposal of data. The data analysis included the importance of quantitative data, the statistical analysis for this study, and the quantitative data analysis process. Then, the section concluded with the ethical considerations of the study.

5.4.4 Chapter 4

This chapter presented the interpretation and discussion of findings after data collection and analysis. The survey responses of this study had a response rate of 120 surveys completed where half of the respondents were males and the other half were females. The survey questionnaires were analysed at the Likert scale and the questions used in the surveys were all deemed reliable. A validity and factor analysis was done to determine whether all questions hold any form of construct validity to measure what it is intended to measure. Also, the data were tested for normality and were discovered to be non-normal distributed data. Non-parametric tests were used to analyze and test the data at mean scores and correlation. Spearman's rho was used to determine the relationship between the technological, organizational, and environmental factors. Also, the Kruskal-Wallis H Test was used to determine the relationship between job position and experience for effective information security adoption in SMEs. Then, a regression analysis was conducted to determine whether an effective information security policy predicts the successful adoption of information security compliance. Lastly, the chapter concludes by providing SMEs with practical recommendations drawn from the analysis of the study.

5.5 Summary of the results

This section of the chapter is to provide a summary of all the results from the analysis presented in Chapter 4 called the interpretation and discussion of findings and how it relates to the study's research objectives.

5.5.1 Survey response

A total of 120 surveys were received from a sample size of 200. The return rate of the surveys was a total of 60%. The data collected from the 120 surveys were used to conduct the study and to complete the data analysis presented in chapter 4.

5.5.2 Biographic information of respondents

Gender: The purpose of requesting the gender of the respondents was to determine in which gender group the respondents of the survey fall and if there was a significant gender difference in small businesses. The gender of respondents had an equal amount of 50% males and 50% females.

Length at the company: The purpose of requesting the respondent's work experience at the company was to determine if their work experience has a significant impact on their information security compliance in the workplace. The majority of the respondents had work experience of 1 to 5 years with a total of 67 respondents.

Job position: The purpose of this question in the survey was to determine the different job position levels of the respondents at SMEs. The majority of the respondents had a job position of being an employee at the SME. A total of 52 respondents indicated this role.

Organization type: The purpose of requesting the organization type in the survey was to determine under which type the SMEs in this study fall. The results indicated that the majority of the respondents work for organizations that offer services to their customers. A total of 38 respondents indicated this organization type.

5.5.3 Characteristics of instrument development

Likert-scale analysis: The survey questionnaire used in this study was measured on the Likert scale. An interval length was used to measure the mean scores in the study. The first interval length started

at 0.80 from the lower limit to the upper limit. The interval length for the level of “Strongly agree” had an interval of [1: 1.80] and “Disagree” had an interval of [1.80: 2.60]. The interval length for the level of “Neutral” had an interval of [2.60: 3.40] and the level of “Agree” has an interval of [3.40: 4.20]. The last interval length at “Strongly agree” has an interval of [4.20: 5].

Reliability analysis: The reliability was measured at internal consistency and used the analysis of Cronbach’s Alpha to determine reliability. A set of 18 questions was used in the survey for the technological factors and the Cronbach’s alpha value was 0.92, which was deemed reliable. There was a set of 24 questions used for the organizational factors and Cronbach’s alpha value was 0.907. This was also deemed reliable. The environmental factors had a set of 18 questions that were used and the Cronbach’s alpha value was 0.907, which was also deemed reliable. This is an indication that all the survey questions used in this study produced internal consistencies higher than 0.90 (exceeding the minimum value of 0.70) which was acceptable for reliability.

Validity and factor analysis: Factor analysis and Kaiser-Meyer-Olkin (KMO) sampling adequacy were used to measure the construct validity of the survey questionnaires. The study found that SMEs’ compliance with information security adoption was influenced by the following factors:

- Section B: Technological factors (Technological compatibility, Existing technology, and Technological complexity)
- Section C: Organizational factors (Top management support, Information security awareness, Policies, and standards, Organizational learning culture)
- Section D: Environmental Factors (Risks in outsourcing, Security and Privacy compliance, Security regulatory concerns)

Test for normality: The normality test was done using the Kolmogorov-Smirnov and the Shapiro-Wilk test for normality. Both tests use an alpha value of 0.05. The KS and SW tests yield significance values less than 0.001. This indicated that the data in this study were not normally distributed and made use of non-parametric tests.

5.5.4 Technological factors

The first factor was identified as the “existing technology” in organizations had a mean score of 3.98 and 0.79 standard deviations. As a result, the majority of respondents believed their innovation and skills impact their compliance with information security policies. The second-highest mean score was

the factor identified as “technological compatibility”. This factor had a mean score of 3.37 and a standard deviation of 0.89. The results indicated that respondents agree that internal information systems applications affect information security compliance. Also, there was a highly statistically significant positive correlation between the two factors called technological compatibility and existing technology, $r(120) = .541^{**}$, $p = .001$. This revealed that the SMEs current security technology fits well with the existing technology setting in the company. Therefore, the results of this study indicated that the technological factors that influence the adoption of information security compliance are existing technology and technological compatibility.

5.5.5 Organizational factors

The first organizational factor was identified as the “organizational learning culture”. This factor had a mean score of 3.32 and a standard deviation of 0.86. Accordingly, the majority of the respondents agreed that learning characteristics and organizational orientation affect information security compliance. The second factor was identified as “policies and standards” and had a mean score of 3.23 with a standard deviation of 0.98. Based on the results, most respondents believe guidelines, procedures, and technical controls specified in InfoSec policies have an impact on information security. In addition, there was a highly statistically significant positive correlation between the factors identified as organizational learning culture and information security policies, $r(120) = .669^{**}$, $p = .001$. This indicated that the employee’s ability to adapt to new technology or innovation causes them to focus more on being compliant with the company’s security policies and standards. Therefore, the results of this study indicated that the organizational factors that influence the adoption of information security compliance are organizational learning culture and information security policies.

5.5.6 Environmental factors

The first environmental factor identified was the “security and privacy compliance” factor which had a mean score of 3.82 and a standard deviation of 0.70. The majority of respondents agreed that they are compliant with the information security policies and standards that are set out by the organization. The second factor was the “security regulations”. This factor had a mean score of 2.65 and a standard deviation of 1.00. This indicated that a majority of respondents have a neutral view that the organizational concerns in ensuring compliance with security and data privacy regulations have an impact on their information security compliance. Therefore, the results of this study reveal that the

environmental factors that influence the adoption of information security compliance are security and privacy compliance and security regulations.

5.5.7 The relationship between the T-O-E factors

There was a high statistically significant correlation between the factors of technological complexity and information security awareness, $r(120) = .773^{**}$, $p = .001$. It suggests that employees' belief in the value of compliance with information security policies and standards is affected by the uncertainty surrounding technology in SMEs. There was a high statistically significant correlation between technological compatibility and security policies and standards, $r(120) = .653^{**}$, $p = .001$. Employees are easily able to adapt to new technologies because SMEs implement information security rules and guidelines. There was a high statistically significant correlation between the factors of technological compatibility and information security awareness, $r(120) = .639^{**}$, $p = .001$. Employees who value information security compliance can adapt to new technology without violating any security policies or standards. There was a high statistically significant correlation between the factors of existing technology and information security awareness, $r(120) = .635^{**}$, $p = .001$. Therefore, management's approach to promoting information security in the workplace will enable employees to use existing technology efficiently. Therefore, the results of this study reveal that there is a positive relationship between the factors called technological complexity, information security awareness, technological compatibility, information security policies, and existing technology.

5.5.8 The relationship between job position and experience with InfoSec Compliance

The results of the Kruskal-Wallis H Test revealed that there was no statistically significant difference between the three groups named job position, experience, and security compliance, $H(3) = 4.926$, $p = 0.177$. Therefore this study reveals that management and employees' experience in their job position does not guarantee that they will comply with the information security policies and standards in the workplace to meet the regulatory requirements.

5.5.9 The successful adoption of InfoSec Compliance

The results revealed that there was a positive statistically significant impact on the successful adoption of InfoSec compliance. Policies and standards predict an impact on compliance behaviour revealed as, $(B1 = .299)$. Considering the results of this study, it can be revealed that the effective use of policies and standards in SMEs leads to the successful adoption of information security compliance.

5.5.10 Practical recommendations for SMEs

In this study, several recommendations were made for SMEs to effectively adapt to information security compliance in the workplace. The recommendations were categorized as technological, organizational, and environmental recommendations.

The technological recommendations were: It is recommended that SMEs make sure that the technology and innovation in the workplace fit well with the employee's skills, values, and previous practices. It is recommended that the management in SMEs implement policies that motivate employees to speak up about the use of complex technology in the workplace. It is recommended that the existing technology setting in SMEs always fit with the intended technology innovation that the organization wishes to adopt.

The organizational recommendations were as follows: It is recommended that SMEs invest in learning capabilities so that they can learn new technology, identify opportunities, provide practical solutions, and have processes in place to scan for risks. It is recommended that SMEs get their management involved in engaging with employees to make sure they understand how crucial information security is in the workplace. It is recommended that SMEs always stay updated on what their employee's needs and challenges are in the workplace. It is recommended that SMEs make sure that their security policies and standards are strong enough to cover the business and its customers.

The environmental recommendations were: It is recommended that SMEs invest in appointing a legal compliance officer to make sure that the organization is compliant with the security laws and regulations. It is recommended that SMEs stay updated on any changes in the law and regulations of information security like the POPI Act. It is recommended that SMEs consider investing in outsourcing their security to a professional and highly recommended security company. This will enable the organization to deal with security professionals that provide solutions and opportunities that benefit the organization's information security policies, standards, and compliance.

5.6 Critical evaluation of the research objectives

This section of the chapter evaluates the success of the study by revisiting the study's objectives.

5.6.1 Objective 1: To determine the technological factors impacting the adoption of information security compliance among SMEs

To achieve this objective, the study measured the survey questionnaires used for the data collection on the Likert scale. The data collected from the Likert scale measurements were used to summarise the data in terms of mean scores and standard deviation which identified the factors. The factors with the highest mean scores and standard deviation were “existing technology” and “technological compatibility”. There was also a high statistically significant positive correlation between the two factors, $r(120) = .541^{**}$, $p = .001$. Therefore, this study identified two technological factors that impact information security compliance among SMEs.

5.6.2 Objective 2: To determine the organizational factors influencing the adoption of information security compliance among SMEs

To achieve this objective, the study measured the survey questionnaires used for the data collection on the Likert scale. The data collected from the Likert scale measurements were used to summarise the data in terms of mean scores and standard deviation which identified the factors. The factors with the highest mean scores and standard deviation were “organizational learning culture” and “policies and standards”. There was also a high statistically significant positive correlation between the factors identified, $r(120) = .669^{**}$, $p = .001$. Therefore, this study identified two organizational factors that impact information security compliance among SMEs.

5.6.3 Objective 3: To determine the environmental factors affecting the adoption of information security compliance among SMEs

To achieve this objective, the study measured the survey questionnaires used for the data collection on the Likert scale. The data collected from the Likert scale measurements were used to summarise the data in terms of mean scores and standard deviation which identified the factors. The factors with the highest mean scores and standard deviation were “security and privacy compliance” and “security and privacy regulations”. Therefore, this study identified two environmental factors that impact information security compliance among SMEs.

5.6.4 Objective 4: To reach conclusions drawn from the research study to make practical recommendations to SMEs.

To achieve this objective, the study draws conclusions from the data analysis in this study and presented in Chapter 4 called the interpretation and discussion of findings. The literature presented in Chapter 2 identified several factors that could be considered in making recommendations. Practical recommendations were presented and discussed in Section 4.9 of Chapter 4.

5.7 Limitations of study

The study focus was restricted to small and medium-sized enterprises in Cape Town which is in the Western Cape region of South Africa. It does not accurately represent the province or the entire nation. Extra caution should be used when interpreting the results and considering recommendations because the results cannot be generalized to other SMEs. Another limitation was that the study was conducted during the COVID-19 pandemic which created some challenges for the SMEs that were initially contacted to partake in the study. Some SMEs unfortunately could not handle the implications of the pandemic and had to close their doors. Therefore, only the SMEs that remained in business continued to take part in the study. Lastly, there is a significant body of literature on information security. Only a few elements/factors that affect SMEs and their information security compliance were studied to reach the research objectives. The objectives that were researched were taken into consideration when interpreting the results and conclusions of this study.

5.8 Contribution of research

Organizations' increasing dependence on information systems has exposed their sensitive information to the danger of cybercrime today (Reddy & Rao, 2016). In light of this, organizations must implement proactive measures to protect organizational information in the dynamic world of today (AlKalbani, Deng, Kam, & Zhang, 2017). A proactive strategy that is frequently utilized is enforcing information security compliance, also known as the application of information security standards and regulations for securing information in businesses (Safa, Von Solms, & Furnell, 2016).

Theoretically, this study contributes to the field of information security compliance research by providing a deeper understanding of the factors that impact SMEs' ability to improve their information security compliance. More practically, this study educates SMEs' information security policy directors on the various recommendations to address these factors as well as provides advantages of outsourcing their information security. In addition, the results of this study

contribute towards improved information security management guidance and compliance for small to medium businesses as well as greater accountability, integrity, and governance among employees.

5.9 Suggestions for future research

To evaluate and assess the ability of the results in this study, a successful route would be to replicate this study in other nations or regions with diverse organizational and cultural environments. To ensure information security compliance in organizations, further research should take psychological factors into account. It is important to research additional categories of factors that affect employee and management adherence to information security regulations. Another angle for future studies is to use alternative research methods for data collection. Interviews and observation will be a great way to engage and observe SMEs. It will assist the researcher to collect “richer information” however it will take a longer time to collect the information.

5.10 Conclusion of study

There are many complexities associated with information security in small and medium-sized businesses (SMEs). SMEs have been able to collect valuable information as a result of the explosive growth of the internet and its related technologies. Due to this, SMEs are vulnerable to cybercrime and information breaches. The respondents in this study acknowledged that they are aware of the technology and systems used in the businesses present risks and challenges for their daily operations. Also, the respondents understood the importance of information security in their business, and why they should comply with regulations. However, several SMEs struggle to comply with the regulations set by the SA government. Thus, different factors have been identified in this study with practical recommendations for SMEs to follow and assist with their InfoSec adoption. Also, positive relationships between the factors identified have been discussed to determine the successful adoption of information security policies (ISP), security standards, and compliance with security and privacy regulations.

References

- Abazi, B. (2018). Risk Assessment process according to the National Institute of Standards and Technology (NIST).
- Abor, J., & Quartey, P. (2010). Issues in SME development in Ghana and South Africa. *International research journal of Finance and Economics*, 39(6), 215-228.
- Abusef, A., & Tarofder, A. K. (2021). Investigating the influencing factors on student's behavioral intention to adopt e-management in Libyan universities. *Journal of Global Business and Social Entrepreneurship (GBSE)*.
- Ahmad Salleh, K., Janczewski, L., & Beltran, F. (2015). SEC-TOE framework: Exploring security determinants in big data solutions adoption. *PACIS 2015 Proceedings*.
- Ahmi, A., Saidin, S. Z., & Abdullah, A. (2014). IT adoption by internal auditors in the public sector: A conceptual study. *Procedia-Social and Behavioral Sciences*, 591-599.
- Ajayi, V. (2017). Primary Sources of Data and Secondary Sources of Data.
- Ajjola, A., Zavarisky, P., & Ruhl, R. (2014). A review and comparative evaluation of forensics guidelines of NIST SP 800-101. *In World Congress on Internet Security (WorldCIS-2014)*, 66-73.
- Al Kilani, M., & Kobziev, V. (2016). An overview of research methodology in information systems (IS). *Open Access Library Journal*, 1-9.
- Alharahsheh, H., & Pius, A. (2020). A review of key paradigms: Positivism VS interpretivism. *Global Academic Journal of Humanities and Social Sciences*, 39-43.
- Alhassan, M. M., & Adjei-Quaye, A. (2017). Information security in an organization. *International Journal of Computer (IJC)*, 100-116.
- Alhogail, A., & Mirza, A. (2014). Information security culture: a definition and a literature review. *In Proceedings of IEEE World Congress On Computer Applications and Information Systems*.
- Ali, A. (2021). Quantitative Data Analysis.
- AlKalbani, A., Deng, H., & Kam, B. (2014). A conceptual framework for information security in public organizations for e-government development. *ACIS*.
- AlKalbani, A., Deng, H., & Kam, B. (2015). Investigating the role of socio-organizational factors in information security compliance in organizations. *Australasian Conference on Information Systems*.
- AlKalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information security compliance in organizations: An institutional perspective. *Data and Information Management*, 104-114.

- Almeida, L., & Respício, A. (2018). Decision support for selecting information security controls. *Journal of Decision Systems*, 173-180.
- Alotaibi, M., Furnell, S., & Clarke, N. (2016). Information security policies: A review of challenges and influencing factors. *In 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 352-358). IEEE.
- Alshamaila, Y., Papagiannidis, S., & Stamati, T. (2013). Cloud computing adoption in Greece. *In UKAIS*, 5.
- Alshenqeti, H. (2014). Interviewing as a data collection method: A critical review. *English linguistics research*, 39-45.
- Aminzade, M. (2018). Confidentiality, integrity, and availability—finding a balanced IT framework. *Network Security*, 9-11.
- Andress, J. (2011). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Elsevier.
- Antwi, S. K., & Hamza, K. (2015). Qualitative and quantitative research paradigms in business research: A philosophical reflection. *European Journal of Business and Management*, 7(3), 217-225.
- Appari, A., Johnson, M. E., & Anthony, D. L. (2009). HIPAA Compliance: An Institutional Theory Perspective. *Proceedings of the 15th Americas Conference on Information Systems*, (pp. 252-261). San Francisco, CA.
- Apuke, O. D. (2017). Quantitative research methods: A synopsis approach. *Kuwait Chapter of Arabian Journal of Business and Management Review*, 1-8.
- Arjaliès, D. L., & Mundy, J. (2013). The use of management control systems to manage CSR strategy: A levers of control perspective. *Management Accounting Research*, 284-300.
- Asah, F., Fatoki, O. O., & Rungani, E. (2015). The impact of motivations, personal values, and management skills on the performance of SMEs in South Africa. *African Journal of Economic and Management Studies*.
- Assante, D., Castro, M., Hamburg, I., & Martin, S. (2016). The use of cloud computing in SMEs. *Procedia computer science*, 38, 1207-1212.
- Aswal, D. K. (2020). Quality infrastructure of India and its importance for inclusive national growth. *MAPAN*, 139-150.
- Ayandibu, A. O., & Houghton, J. (2017). The role of Small and Medium Scale Enterprise in local economic development (LED). *Journal of Business and Retail Management Research*, 11(2).
- Azungah, T. (2018). Qualitative research: deductive and inductive approaches to data analysis. *Qualitative research journal*.

- Babbie, E. (2021). *The practice of social research*. Boston, MA: Cengage.
- Baker, J. (2012). The technology–organization–environment framework. *Information systems theory*, 231-245.
- Baker, W. H., & Wallace, L. (2007). Is information security under control?: Investigating quality in information security management. *IEEE Security & Privacy*, 36-44.
- Bala, J. (2016). Contribution of SPSS in Social Sciences Research. *International Journal of Advanced Research in Computer Science*, 6.
- Battistella, C., De Toni, A. F., & Pillon, R. (2016). Inter-organisational technology/knowledge transfer: a framework from critical literature review. *The Journal of Technology Transfer*, 1195-1234.
- Bell, N. (2008). Ethics in child research: rights, reason and responsibilities. *Children's Geographies*, 6(1), 7-20.
- Bhaskar, S. M., & Ahson, S. I. (2008). *Information Security: A Practical Approach*. Oxford: Alpha Science International Ltd.
- Biddle, C., & Schafft, K. A. (2015). Axiology and anomaly in the practice of mixed methods work: Pragmatism, valuation, and the transformative paradigm. *Journal of Mixed Methods Research*, 320-334.
- Borgman, H. P., Bahli, B., Heier, H., & Schewski, F. (2013). Cloudrise: exploring cloud computing adoption and governance with the TOE framework. In *2013 46th Hawaii international conference on system sciences* (pp. 4425-4435). IEEE.
- Botha, J. G., Eloff, M. M., & Swart, I. (2015). The effects of the PoPI Act on small and medium enterprises in South Africa. In *2015 Information Security for South Africa (ISSA)* (pp. 1-8). IEEE.
- Bowden, A., Fox-Rushby, J. A., Nyandieka, L., & Wanjau, J. (2002). Methods for pre-testing and piloting survey questions: illustrations from the KENQOL survey of health-related quality of life. *Health policy and planning*, 17(3), 322-330.
- Brace, I. (2004). *Questionnaire Design Survey Material for Effective. Business. Viitattu*, 28, p.2018. (28 ed.). Viitattu: Business.
- Bratt, M. (2018). *Information Regulator happy with Liberty's conduct over data breach*. The media online.
- Brown, S., Gommers, J., & Serrano, O. (2015). From cyber security information sharing to threat management. In *Proceedings of the 2nd ACM workshop on information sharing and collaborative security*, 43-49.

- Bruening, P. J., Sotto, L. J., Abrams, M. E., & Cate, F. H. (2008). Strategic information management. *Privacy and Security Law Report*, 1361-1363.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 523-548.
- Bunker, G. (2012). Technology is not enough: Taking a holistic view for information assurance. *Information Security Technical Report*, 17(1-2), 19-25.
- Burmeister, F., Drews, P., & Schirmer, I. (2019). A privacy-driven enterprise architecture meta-model for supporting compliance with the general data protection regulation. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 6052-6061.
- Butler, T. (2011). Compliance with institutional imperatives on environmental sustainability: Building theory on the role of Green IS. *The Journal of Strategic Information Systems*, 6-26.
- Bvuma, S., & Marnewick, C. (2020). Sustainable livelihoods of township small, medium, and micro enterprises towards growth and development. *Sustainability*, 12(8), 3149.
- Calland, R., & Tilley, A. (2018). *SA waits on the information regulator*.
- Calzon, B. (2020). *Your Modern Business Guide To Data Analysis Methods And Techniques*. Retrieved from The Datapine Blog: <https://www.datapine.com/blog/data-analysis-methods-and-techniques/>
- Cavalluzzo, K. S., & Ittner, C. D. (2004). Implementing performance measurement innovations: evidence from the government. *Accounting, Organizations and Society*, 243-267.
- Cavusoglu, H., Son, J., & Benbasat, I. (2015). Institutional Pressures in Security Management: Direct and Indirect Influences on Organizational Investment in Information Security Control Resources. *Information & Management*, 52, 385-400.
- Chauke, K. R. (2019). Critical analysis of principle one and two of king iv report on corporate governance: leadership and ethics. *International Conference on Public Administration and Development Alternatives (IPADA)*.
- Chen, H., & Li, W. (2014). Understanding organization employees information security omission behavior: An integrated model of social norm and deterrence.
- Chen, H., Chau, P. Y., & Li, W. (2018). The effects of moral disengagement and organizational ethical climate on insiders' information security policy violation behavior. *Information Technology & People*.
- Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile networks and applications*, 171-209.

- Chipperfield, C., & Furnell, S. (2010). From security policy to practice: Sending the right messages. *Computer Fraud & Security, Elsevier Ltd*, 13-19.
- Coderre, D., & Police, R. C. (2005). Global technology audit guide: continuous auditing implications for assurance, monitoring, and risk assessment. *The Institute of Internal Auditors*, 1-34.
- Coetzee, J. (2004). The Electronic Communications and Transactions Act 25 of 2002: facilitating electronic commerce. *Stellenbosch Law Review*, 501-521.
- Constitution of the Republic of South Africa No 108*. RSA. (1996).
- Cooper, R. B., & Zmud, R. W. (1990). Information technology implementation research: a technological diffusion approach. *Management Science*, 123-139.
- Correia, A., Gonçalves, A., & Teodoro, M. F. (2017). A model-driven approach to information security compliance. *In AIP Conference Proceedings* (p. 020082). AIP Publishing LLC.
- Creswell, J. W., & Plano Clark, V. L. (2007). *Designing and conducting mixed methods research*. Thousand Oaks, CA: Sage Publications.
- Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 297-334.
- Crossley, J. (2021). How To Write The Conclusion Chapter. Florida: GradCoach International.
- Cumbly, R., & Church, P. (2013). Is “big data” creepy? *Computer Law & Security Review*, 601-609.
- Cyber Security Framework*. (2018). Retrieved from Sogeti Labs: <https://labs.sogeti.com/cyber-security-framework-healthcare/>
- Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, 234-256.
- Dala, P., & Venter, H. S. (2016). Understanding the level of compliance by South African institutions to the Protection of Personal Information (POPI) Act. *In Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists*, (pp. 1-8).
- D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of management information systems*, 285-318.
- Das, S., Kundu, A., & Bhattacharya, A. (2020). Technology adaptation and survival of SMEs: a longitudinal study of developing countries. *Technology Innovation Management Review*.
- Davenport, T., & Prusak, L. (1998). *Working knowledge: how organizations manage what they know*. Cambridge, MA: Harvard Business School Press.
- David, B., & Resnik, J. (2011). What is Ethics in Research & Why is it Important? *National Institute of Environmental Health Sciences*, 1-10.

- De Bruyn, M. (2014). The protection of personal information (POPI) Act: impact on South Africa. *International Business & Economics Research Journal*.
- de Oliveira Albuquerque, R., García Villalba, L. J., Orozco, A. L., Buiati, F., & Kim, T. (2014). A layered trust information security architecture. *Sensors*, 22754-22772.
- Diamantopoulou, V., Tsohou, A., & Karyda, M. (2019). From ISO/IEC 27002: 2013 information security controls to personal data protection controls: guidelines for GDPR compliance. *In Computer Security* (pp. 238-257). Springer.
- Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). *Internet, phone, mail, and mixed-mode surveys: The tailored design method*. John Wiley & Sons.
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American sociological review*, 147-160.
- DiMase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environment Systems and Decisions*, 291-300.
- Doherty, N. F., & Tajuddin, S. T. (2018). Towards a user-centric theory of value-driven information security compliance. *Information Technology & People*.
- Dörnyei, Z., & Csizér, K. (2012). How to design and analyze surveys in second language acquisition research. *Research methods in second language acquisition: A practical guide*, 74-94.
- Drucker, P. (2001). The next society. *The economist*.
- Efrat, K., Hughes, P., Nemkova, E., & Souchon, A. L. (2018). Leveraging of Dynamic export capabilities for competitive advantage and performance consequences: Evidence from China. *Journal of Business Research*, 114-124.
- Eiselen, S. (2014). Fiddling with the ECT act—Electronic signatures. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, 2805-2820.
- Electronic Communications and Transactions Act 25*. (2002).
- Electronic Communications and Transactions Amendment Bill*. (2012).
- Evans, O., Josephine, P., & Yeboah, O. (2015). Challenges faced by SMEs in accessing credit in Tamale. *Global Journal of Commerce and Management Perspective*, 4(5), 32-39.
- Fay, J. J., & Patterson, D. (2018). Chapter 24 - The Importance of Policies and Procedures. *In Contemporary Security Management*. Butterworth-Heinemann.
- Fazlida, M. R., & Said, J. (2015). Information security: Risk, governance and implementation setback. *Procedia Economics and Finance*, 243-248.
- Ferguson, C. S. (2019). Assessing the KING IV Corporate Governance Report in relation to business continuity and resilience. *Journal of Business Continuity & Emergency Planning*, 174-185.

- Flanagin, A. J. (2000). Social pressure on organizational website adoption. *Human Communication Research*, 618-646.
- Fouad, M. A. (2013). Factors affecting the performance of small and medium enterprises (SMEs) in the manufacturing sector of Cairo, Egypt. *International Journal of business and management studies*, 157-166.
- Frank, I. E., & Todeschini, R. (1994). *The data analysis handbook*. Elsevier.
- Fruhlinger, J. (2020, February 10). *The CIA triad: Definition, components, and examples*. Retrieved from CSO: <https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html>
- Frühwirth, C. (2009). On business-driven it security management and mismatches between security requirements in firms, industry standards, and research work. *In International Conference on Product-Focused Software Process Improvement* (pp. 375-385). Berlin: Springer.
- Fugard, A. J., & Potts, H. W. (2015). Supporting thinking on sample sizes for thematic analyses: a quantitative tool. *International Journal of Social Research Methodology*, 669-684.
- Gangwar, H., Date, H., & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *Journal of Enterprise Information Management*, 107-130.
- Gibbert, M., Leibold, M., & Probst, G. (2002). Five styles of customer knowledge management, and how smart companies use them to create value. *European management journal*, 459-469.
- Gladden, M. E. (2017). *The Handbook of Information Security for Advanced Neuroprosthetics*. Synthypnion Academic. *Synthypnion Academic*.
- Glasow, P. (2005). *Fundamentals of Survey Research Methodology*. Washington State: Distribution unlimited.
- Goertzen, M. J. (2017). Introduction to quantitative research and data. *Library Technology Reports*, 53(4), 12-18.
- Goldstein, J., Chernobai, A., & Benaroch, M. (2011). An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories. *Journal of the Association for Information Systems*, 606-631.
- Goundar, S. (2012). *Chapter 3 - Research Methodology and Research Method*. Victoria: University of Wellington.
- Halawani, F., & Rahman, M. S. (2013). A Proposed Framework for E-Commerce Usage and Competitive Advantage on Small and Medium Tourism Enterprises (SMTES) in Lebanon. *Journal of Social and Development Sciences*, 258-267.

- Harcourt, M., Lam, H., & Harcourt, S. (2005). Discriminatory practices in hiring: Institutional and rational economic perspectives. *The International Journal of Human Resource Management*, 2113-2132.
- Haris, A. R., Sarijan, S., & Hussin, N. (2017). Information security challenges: a Malaysian context. *International Journal of Academic Research in Business and Social Sciences*, 397-403.
- Harraf, A., Wanasika, I., Tate, K., & Talbott, K. (2015). Organizational agility. *Journal of Applied Business Research (JABR)*, 675-686.
- Hashem, I. A., Yaqoob, I., Anuar, N. B., & Mokhtar, S. (2015). The rise of “big data” on cloud computing: Review and open research issues. *Information systems*, 98-115.
- Hassan, N. K., Mingers, J., & Stahl, B. (2018). Philosophy and information systems: where are we and where should we go? *European Journal of Information Systems*, 27(3), 263-277.
- Heale, R., & Twycross, A. (2015). Validity and Reliability in Quantitative Studies. *Evid Based*.
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organizations. *European Journal of information systems*, 106-125.
- Herrington, M., Kew, P., & Mwanga, A. (2017). *South Africa Report*.
- Hox, J. J., & Boeijs, H. R. (2005). Data collection, primary versus secondary.
- Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, 282-293.
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 83-95.
- Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, 69-79.
- Information Regulator*. (2017, March 200 02). Retrieved from Political Funding Bill_16: <http://www.justice.gov.za/infoereg/index.html>.
- Ishak, N. M., & Abu Bakar, A. Y. (2014). Developing Sampling Frame for Case Study: Challenges and Conditions. *World Journal of Education*, 29-35.
- Islam, T., Khan, S. U., Ahmad, U. N., & Ahmed, I. (2013). “Organizational learning culture and leader-member exchange: the way to enhance organizational commitment and reduce turnover intentions”. *The Learning Organization*, 322-337.
- ISO/IEC 27002:2013*. (2013). Retrieved from ISO: <https://www.iso.org/standard/54533.html>
- Jagadish, H. V., Gehrke, J., Labrinidis, A., Papakonstantinou, Y., Patel, J. M., Ramakrishnan, R., & Shahabi, C. (2014). Big data and its technical challenges. *Communications of the ACM*, 86-94.

- Jan, P. T., Lu, H. P., & Chou, T. C. (2012). The adoption of e-learning: An institutional theory perspective. *Turkish Online Journal of Educational Technology-TOJET*, 326-343.
- John, O. P., & Soto, C. J. (2007). *The importance of being valid: Reliability and the process of construct validation*. New York: Guilford.
- Kabir, S. M. (2016). *Methods of data collection*.
- Kajava, J., Anttila, J., Varonen, R., Savola, R., & Röning, J. (2007). Senior executives' commitment to information security—from motivation to responsibility Computational Intelligence and Security. *Computational Intelligence and Security*, 833-838.
- Kamunge, M. S., Njeru, A., & Tirimba, O. I. (2014). Factors affecting the performance of small and micro enterprises in Limuru Town Market of Kiambu County, Kenya. *International journal of scientific and research publications*, 1-20.
- Kashi, K., Zheng, C., & Molineux, J. (2016). Exploring factors driving social recruiting: The case of Australian organizations. *Journal of Organizational Computing and Electronic Commerce*, 203-223.
- Kaushik, V., & Walsh, C. A. (2019). Pragmatism as a research paradigm and its implications for social work research. *Social sciences*, 255.
- Kent, C., Tanner, M., & Kabanda, S. (2016). How South African SMEs address cyber security: The case of web server logs and intrusion detection. In *2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)*, 100-105.
- Khan, S. N. (2014). Qualitative research method: Grounded theory. *International Journal of Business and Management*, 9(11), 224-233.
- Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. *The Scientific World Journal*.
- Kim, S. S., & Kim, Y. J. (2017). The effect of compliance knowledge and compliance support systems on information security compliance behavior. *Journal of Knowledge Management*.
- Kirsch, L., & Boss, S. (2007). The last line of defense: motivating employees to follow corporate security guidelines. *ICIS 2007 proceedings*, 103.
- Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security*, 24-36.
- Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security*, 3-11.
- Kshetri, N. (2014). Big data impact on privacy, security, and consumer welfare. *Telecommunications Policy*, 1134-1145.

- Lautenbach, P., Johnston, K., & Adeniran-Ogundipe, T. (2017). Factors influencing business intelligence and analytics usage extent in South African organizations. *South African Journal of Business Management*, 48(3), 23-33.
- Laybats, C., & Tredinnick, L. (2016). Information security. *Business Information Review*, 76-80.
- Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, 60-70.
- Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, 707-718.
- Leech, N., Barrett, K., & Morgan, G. A. (2013). *SPSS for intermediate statistics: Use and interpretation*. Routledge.
- Leithwood, K., & Louis, K. S. (2021). *Organizational learning in schools*. Taylor & Francis.
- Leung, D., Lo, A., Fong, L. H., & Law, R. (2015). Applying the Technology-Organization-Environment framework to explore ICT initial and continued adoption: An exploratory study of an independent hotel in Hong Kong. *Tourism Recreation Research*, 391-406.
- Leung, S. (2012). Cyber security risks and mitigation for SME. *CISSP CISA CBCP*, 1-50.
- Levy, P. S., & Lemeshow, S. (2013). *Sampling of populations: methods and applications*. John Wiley & Sons.
- Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of Enterprise Systems: the Effect of Institutional Pressures and the Mediating Role of Top Management. *MIS Quarterly*, 59-87.
- Loia, V., D'Aniello, G., Gaeta, A., & Orciuoli, F. (2016). Enforcing situation awareness with granular computing: a systematic overview and new perspectives. *Granular Computing*, 127-143.
- Luna-Reyes, L. F., & Gil-Garcia, J. R. (2011). Using institutional theory and dynamic simulation to understand complex e-Government phenomena. *Government Information Quarterly*, 329-345.
- Lundgren, B., & Möller, N. (2014). Defining information security. *Science and engineering ethics*, 25(2), 419-447.
- Mabeka, N. Q. (2021). An analysis of the implementation of the caselines system in South African courts in the light of the provisions of section 27 of the electronic communications and transactions act 25 of 2002: a beautiful dream to come true in civil procedure. *Potchefstroom Electronic Law Journal (PELJ)*, 1-31.
- Mahembe, E. (2011). Literature Review on Small and Medium Enterprises Access to Credit and Support in South Africa. *Underhill Corporate Solutions National Credit Regulator (NCR): Pretoria, South Africa*.

- Manzoor, F., Wei, L., & Sahito, N. (2021). The role of SMEs in rural development: Access of SMEs to finance as a mediator. *PLoS One*, *16*(3), 1.
- Maritz, M. J., & Hattingh, V. (2015). Electronic communication in the construction industry. *Journal of Engineering, Design, and Technology*, 74-93.
- Matandela, W. (2017). *Determinants Influencing Adoption of Cloud Computing by Small Medium Enterprises in South Africa*. University of the Witwatersrand.
- Mathiyazhagan, T., & Nandan, D. (2017). *Survey Research Method*. Washington State: Distribution unlimited.
- McCrae, R. R., Kurtz, J. E., Yamagata, S., & Terracciano, A. (2011). Internal consistency, retest reliability, and their implications for personality scale validity. *Personality and social psychology review*, 28-50.
- McIlwraith, A. (2006). *Information security and employee behaviour: how to reduce risk through employee education, training, and awareness*. Gower Publishing, Ltd.
- Meriah, I., & Rabai, L. B. (2019). Comparative study of ontologies based iso 27000 series security standards. *Procedia Computer Science*, 85-92.
- Merkow, M. S., & Breithaupt, J. (2014). *Information security: Principles and practices*. Pearson Education.
- Metaxiotis, K. (2009). Exploring the rationales for ERP and knowledge management integration in SMEs. *Journal of Enterprise Information Management*, 51-62.
- Mitchell, C. (2015). Privacy, compliance, and the cloud. *Guide to Security Assurance for Cloud Computing*, 3-14.
- Moghavvemi, S., Salleh, N. A., Sulaiman, A., & Abessi, M. (2015). Effect of external factors on intention–behaviour gap. *Behaviour & Information Technology*, 1171-1185.
- Mohajan, H. K. (2017). Two criteria for good measurements in research: Validity and reliability. *Annals of Spiru Haret University*, *17*(4), 59-82.
- Morin, J. H., Aubert, J., & Gateau, B. (2012). Towards cloud computing SLA risk management: issues and challenges. In *2012 45th Hawaii International Conference on System Sciences* (pp. 5509-5514). IEEE.
- Mukherjee, I., & Paul, G. (2013). Efficient multi-bit image steganography in spatial domain. In *International Conference on Information Systems Security* (pp. 270-284). Berlin, Heidelberg: Springer.
- Muriithi, S. M. (2017). African small and medium enterprises (SMEs) contributions, challenges, and solutions.

- Mutalemwa, D. K. (2015). Does globalisation impact SME development in Africa? *African Journal of Economic and Management Studies*, 164-182.
- Nardi, P. M. (2018). *Doing survey research: A guide to quantitative methods*. Routledge.
- Nassimbeni, G., Sartor, M., & Dus, D. (2012). *Security risks in service offshoring and outsourcing*. Retrieved from <http://www.emeraldinsight.com/doi/abs/10.1108/02635571211210059>
- Ncube, T., & Zondo, D. (2022). Entrepreneurial Attributes responsible for Small and Medium Enterprise Growth in South Africa: Small and Medium Enterprise Owners' perspectives. *International Journal of Special Education*, 37, 2022-8223.
- Ndolo, A., Ogara, S. O., & Liyala, S. (2018). Model for information security governance prediction in public Universities in Kenya. *International Journal of Computer Applications Technology and Research*, 63-77.
- Nikander, J., Manninen, O., & Laajalahti, M. (2020). Requirements for cybersecurity in agricultural communication networks. *Computers and Electronics in Agriculture*.
- NIST Special Publication 800-series General Information*. (2018). Retrieved from NIST: <https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information>
- Odor, H. O. (2018). A literature review on organizational learning and learning organizations. *International Journal of Economics & Management Sciences*, 1-6.
- Oláh, J., Kitukutha, N., Haddad, H., & Pakurár, M. (2018). Achieving sustainable e-commerce in environmental, social, and economic dimensions by taking possible trade-offs. *Sustainability*, 89.
- Olawale, F., & Garwe, D. (2010). Obstacles to the Growth of New SMEs in South Africa: A principal Component Analysis Approach. *African Journal of Business Management*, 4(5), 729-738.
- Oliveira, T., Thomas, M., & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. *Information & Management*, 497-510.
- Orna, E. (2004). *Information Strategy in Practice*. Routledge.
- Pasquier, T., Singh, J., Eysers, D., & Bacon, J. (2015). CamFlow: Managed data-sharing for cloud services. *IEEE Transactions on Cloud Computing*, 472-484.
- Pearson, S., & Benameur, A. (2010). Privacy, security, and trust issues arising from cloud computing. *In 2010 IEEE Second International Conference on Cloud Computing Technology and Science* (pp. 693-702). IEEE.

- Piggin, R. S. (2013). Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security. *In IET conference on control and automation 2013: Uniting problems and solutions* (pp. 1-6). IET.
- Polit, D. F. (2015). Assessing measurement in health: Beyond reliability and validity. *International Journal of nursing studies*, 1746-1753.
- Protection of Personal Information Act 4*. (2013).
- Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *Mis Quarterly*, 757-778.
- PwC. (2016). *A summary of the King IV Report on Corporate Governance™ for*. Retrieved from PwC: <https://www.pwc.co.za/kingIV>
- Qadir, S., & Quadri, S. M. (2016). Information availability: An insight into the most important attribute of information security. *Journal of Information Security*, 185-194.
- Rainer, & Cegielski. (2010). *Introduction to Information System: Enabling and Transformation of Business. 3rd Edition Wiley and Sons.*
- Ramukumba, T. (2014). Overcoming SMEs challenges through critical success factors: A case of SMEs in the Western Cape Province, South Africa. *Economic and business review*, 16(1), 19-38.
- Redman, T. C. (2008). *Data driven: profiting from your most important business asset.* Harvard Business Press. *Harvard Business Press.*
- Rehman, A. A., & Alharthi, K. (2016). An Introduction to Research Paradigms. *International Journal of Educational Investigations*, 3(8), 51-53.
- Republic of South Africa. (2013). *“Protection of Personal Information (POPI) Act (Act 4 of 2013)”*. Cape Town: Government Printer.
- Research Onion - Explanation of the Concept. (2018). *UKEssays*. Retrieved from <https://www.ukessays.com/essays/psychology/explanation-of-the-concept-of-research-onion-psychology-essay.php?vref=1>
- Ridley, D. (2012). *The literature review: A step-by-step guide for students.* New York: SAGE Publications.
- Ritella, G., Rajala, A., & Renshaw, P. (2020). Using chronotype to research the space-time relations of learning and education: Dimensions of the unit of analysis. *Learning, Culture and Social Interaction*, 31, p.100381.
- Ritter, A., & Munoz-Carpena, R. (2013). Performance evaluation of hydrological models: Statistical significance for reducing subjectivity in goodness-of-fit assessments. *Journal of Hydrology*, 33-45.

- Rogers, E. M. (2003). *Diffusion of innovations*. New York: Free Press: Free Press.
- Rungani, E. C., & Potgieter, M. (2018). The impact of financial support on the success of small, medium, and micro enterprises in the Eastern Cape province. *Acta Commercii*, 18(1), 1-12.
- Ruwanza, S., & Shackleton, C. M. (2016). Incorporation of environmental issues in South Africa's municipal Integrated Development Plans. *International journal of sustainable development & world ecology*. *International journal of sustainable development & world ecology*, 28(1), 28-39.
- Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 70-82.
- Sahin, I. (2006). Detailed review of Rogers' diffusion of innovations theory and educational technology-related studies based on Rogers' theory. *Turkish Online Journal of Educational Technology-TOJET*, 14-23.
- Saint-Onge, H. (2002). Linking knowledge to strategy. *In Strategic Planning for KM Conference*, 28-29.
- Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, 89.
- Salleh, K. A., & Janczewska, L. (2016). Technological, organizational and environmental security and privacy issues of big data: A literature review. *Procedia Computer Science*, 100, 19-28.
- Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity, and availability in security. *Journal of Information System Security*, 10(3), 21-45.
- Sattarova Feruza, Y., & Kim, T. H. (2007). IT security review: Privacy, protection, access control, assurance, and system security. *International journal of multimedia and ubiquitous engineering*, 17-32.
- Saunders, M. N., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students* (8th ed.). United Kingdom: Pearson Education Limited.
- Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research methods for Business Students* (4 ed.). England: Pearson Education Limited.
- Sawicki, V., Wegener, D. T., Clark, J. K., & Fabriga, L. R. (2013). Feeling conflicted and seeking information: When ambivalence enhances and diminishes selective exposure to attitude-consistent information. *Personality and Social Psychology Bulletin*, 735-747.
- Schweitzer, J. A. (1990). *Managing Information Security: Administrative, Electronics, and Legal measures to Protect Business Information*. Boston: Butterworths.
- Scotland, J. (2012). Exploring the philosophical underpinnings of research: Relating ontology and epistemology to the methodology and methods of the scientific, interpretive, and critical research paradigms. *English language teaching*, 9-16.

- Sedgwick, P. (2014). Cluster randomised controlled trials. *BMJ*.
- Sekgweleo, T., & Mariri, M. (2019). Critical analysis of the PoPI Act within the organisation. *International Journal of Computer Science and Information Security (IJCSIS)*.
- Senarathna, I., Wilkin, C., Warren, M., & Yeoh, W. (2018). Factors that influence adoption of cloud computing: An empirical study of Australian SMEs. *Australasian Journal of Information Systems*, 22. *Australasian Journal of Information Systems*, 22.
- Sharma, B. (2016). A focus on reliability in developmental research through Cronbach's Alpha among medical, dental, and paramedical professionals. *Asian Pacific Journal of Health Sciences*, 271-278.
- Shi, W., Shambare, N., & Wang, J. (2008). The adoption of internet banking: An institutional theory perspective. *Journal of Financial Services Marketing*, 272-286.
- Shoufan, A., & Damiani, E. (2017). On inter-rater reliability of information security experts. *Journal of information security and applications*, 101-111.
- Singh, H. P., & Alshammari, T. S. (2020). An Institutional Theory Perspective on Developing a Cyber Security Legal Framework: A Case of Saudi Arabia. *Beijing L. Rev*, 11, 637.
- Smith, S., & Jamieson, R. (2006). Determining Key Factors in E-Government Information System Security. *Information Systems Management*, 23-32.
- Snyman, S. (2014). The impact of ecotourism employment on rural household incomes and social welfare in six southern African countries. *Tourism and Hospitality Research*, 37-52.
- Snyman, S. L. (2012). The role of tourism employment in poverty reduction and community perceptions of conservation and tourism in southern Africa. *Journal of Sustainable Tourism*, 20(3), 395-416.
- Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*.
- Stein, P. (2012). "South Africa's EU-style Data Protection Law". *Without Prejudice*, 48-49.
- Suen, L. J., Huang, H. M., & Lee, H. H. (2014). A comparison of convenience sampling and purposive sampling. *Hu Li Za Zhi*, 61(3), 105. *Hu Li Za Zhi*, 61(3), 105.
- Sulayman, M., Urquhart, C., Mendes, E., & Seide, S. (2012). Software process improvement success factors for small and medium Web companies: A qualitative study. *Information and Software Technology*, 54, 479-500.
- Swartz, P., & Da Veiga, A. (2016). PoPI Act-opt-in and opt-out compliance from a data value chain perspective: A South African insurance industry experiment. *In 2016 Information Security for South Africa (ISSA)* (pp. 9-17). IEEE.

- Symantec. (2015). An Internet of Things reference architecture.
- Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, 9493-9532.
- Taherdoost, H. (2016). Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. *International Journal of Academic Research in Management (IJARM)*, 5(2), 18-27.
- Taherdoost, H. (2016). Validity and Reliability of the Research Instrument; How to Test the Validation of a Questionnaire/Survey in a Research. *International Journal of Academic Research in Management*, 5, 28-36.
- Tchernykh, A., Schwiegelsohn, U., Talbi, E. G., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*, 100581.
- Teo, H. H., Wei, K. K., & Benbasa, I. (2003). Predicting intention to adopt inter-organizational linkages: An institutional perspective. *MIS Quarterly*, 19-49.
- Teo, T. S., Ranganathan, C., & Dhaliwal, J. (2006). Key dimensions of inhibitors for the deployment of web-based business-to-business electronic commerce. *IEEE Transactions on engineering Management*, 395-411.
- Thesismind. (2019). *Analysis of Saunders research onion*. Retrieved from <https://thesismind.com/analysis-of-saunders-research-onion/>
- Thomas, D. R. (2006). A general inductive approach for analysing qualitative evaluation data. *American Journal of Evaluation*, 237-246.
- Thomson Reuters. (2021). *Understanding data privacy: A compliance strategy can mitigate cyber threats*. Retrieved from Thomson Reuters: <https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-a-compliance-strategy-can-mitigate-cyber-threats#:~:text=A%20privacy%20compliant%20organization%20provides,or%20inappropriate%20access%20to%20data.>
- Titus. (2011). "Protecting Personally Identifiable Information (PII) with Classification and Content Inspection". *Titus White Paper*, 5.
- Tofan, D. C. (2011). Information security standards. *Journal of Mobile, Embedded and Distributed Systems*, 128-135.
- Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. MA: Lexington Books.

- Tseng, K. M., & Johnsen, R. E. (2011). Internationalisation and the internet in UK manufacturing SMEs. *Journal of Small Business and Enterprise Development*.
- Tubbs, B. B. (2020). *How companies can gear up for POPI*. Retrieved from IT Web Financial: <http://www.itweb.co.za/?id=71803:How-companies-can-gear-up-for-POPI>.
- Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & health sciences*, 398-405.
- Wall, D. (2007). *Cybercrime: The transformation of crime in the information age*. Polity.
- Wang, S., & Cheung, W. (2004). E-business adoption by travel agencies: prime candidates for mobile e-business. *International Journal of Electronic Commerce*, 43-63.
- Wang, Y., Wei, J., & Vangury, K. (2014). Bring your own device security issues and challenges. *In 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)* (pp. 80-85). IEEE.
- Wedawatta, G., Ingirige, B., & Amaratung, D. (2011). Case study as a research strategy: Investigating extreme weather resilience of construction SMEs in the UK.
- Wen, K. W., & Chen, Y. (2010). E-business value creation in Small and Medium Enterprises: A US study using the TOE framework. *International Journal of Electronic Business*, 80-100.
- Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security 4th edition*. Cengage Learning.
- Winne, P. H., Nesbit, J. C., & Popowich, F. (2017). Study: A system for researching information problem solving. *Technology, Knowledge and Learning*, 22(3), 369-376.
- Xiang, Z., Magnini, V. P., & Fesenmaier, D. R. (2015). Information technology and consumer behavior in travel and tourism: Insights from travel planning using the internet. *Journal of retailing and consumer services*, 244-249.
- Yaokumah, W. (2017). Modelling the impact of administrative access controls on technical access control measures. *Information Resources Management Journal (IRMJ)*, 53-70.
- YAU, H. K. (2014). Information security controls. *Advances in Robotics & Automation*, 100-118.
- Zhao, Y. (2015). *CFI's guide to Data Analysis*. Retrieved from Corporate Finance Institute: <https://corporatefinanceinstitute.com/resources/knowledge/data-analysis/data-analysis/>
- Zheng, D., Chen, J., Huang, L., & Zhang, C. (2013). E-government adoption in public administration organizations: integrating institutional theory perspective and resource-based view. *European Journal of Information Systems*, 221-234.

- Zhu, K., Kraemer, K. L., & Dedrick, J. (2004). Information technology payoff in e-business environments: An international perspective on value creation of e-business in the financial services industry. *Journal of management information systems*, 17-54.
- Ziemba, E., Papaj, T., & Zelazny, R. (2013). A Model of Success Factors for E-Government Adoption—The Case of Poland. *Issues in Information Systems*, 87-100.
- Zvitambo, K., & Chazireni, B. (2019). Driving sustainable growth through humanistic social responsibility in small and medium enterprises of developing countries.

APPENDIX A: Ethical Clearance Certificate



UNIVERSITY of the
WESTERN CAPE



17 July 2020

Ms FL Lawrence
Information Systems
Faculty of Economic and Management Sciences

Ethics Reference Number: HS20/5/18

Project Title: Factors affecting information security compliance among SMEs in Cape Town.

Approval Period: 16 July 2020 – 16 July 2023

I hereby certify that the Humanities and Social Science Research Ethics Committee of the University of the Western Cape approved the methodology and ethics of the above mentioned research project.

Any amendments, extension or other modifications to the protocol must be submitted to the Ethics Committee for approval.

Please remember to submit a progress report by 30 November each year for the duration of the project.

The permission to conduct the study must be submitted to HSSREC for record keeping purposes.

The Committee must be informed of any serious adverse event and/or termination of the study.

A handwritten signature in black ink, appearing to read 'Josias'.

Ms Patricia Josias
Research Ethics Committee Officer
University of the Western Cape

Director: Research Development
University of the Western Cape
Private Bag 8 17
Bellville 7535
Republic of South Africa
Tel: +27 21 959 6111
Email: research-ethics@uwc.ac.za

HSSREC Registration Number: HSSREC-170416-049



UNIVERSITY OF THE WESTERN CAPE
Faculty of Economic and Management Sciences
Department of Information Systems

APPENDIX B: Participation information sheet for SMEs in Cape Town

RESEARCH TITLE: Factors affecting information security compliance among SMEs in Cape Town.

Dear Participant

You are invited to participate in a research study conducted by **Felencia Linthea Lawrence** and Student Number: **3329196**. It is in partial completion of the researcher's thesis toward a Master's degree in the Information systems department, at the University of the Western Cape.

Before you decide to participate, you need to understand the purpose of the research and what it would entail. Please take the time to read the following information carefully and discuss it with others if you wish. If you are unclear about anything, I would be happy to answer any questions you may have.

PURPOSE OF THE STUDY

The purpose of this study is to contribute to information security research by better understanding the importance of information security compliance in SMEs and what framework can assist in the adoption of information security compliance. To achieve this, the study will explore factors affecting information security compliance adoption by giving SMEs some insight as to what is needed in the organization to be compliant with information security policies and standards.

DESCRIPTION OF STUDY AND YOUR INVOLVEMENT

The paper presents a descriptive study to explore what are the factors affecting the adoption of information security compliance among SMEs in Cape Town. Your involvement will contribute to the gathering of primary data through survey questionnaires which will be helpful to create a better understanding of information security compliance adoption among SMEs. The survey questionnaires will take approximately 20 minutes to complete.



CONFIDENTIALITY & ANONYMITY

Please be advised that the results of the study will neither divulge the organization's particulars nor the individual particulars, to maintain confidentiality at all times. Any information that can connect the responses to an individual or organization will remain confidential and will be disclosed only with your permission. The researcher shall keep all records and tapes of your participation, including a signed consent form which is required from you should you agree to participate in this research study, locked away at all times.

(Example: All the data will be kept in password-protected computer files known only to the researcher. Data collection questionnaires will be kept safely in a lockable filing cabinet accessed only by the researcher. All raw data including written documents will be destroyed after three months of the final dissertation being marked and graded. If we write a report or article about this research project, your identity will be protected.)

RISKS OF THE RESEARCH?

There are no risks to participating in this research as I shall take all necessary measures to ensure the overall physical and psychological safety of all respondents. I will uphold the ethical values of voluntary participation, avoid all forms of harm, and deception, ensure the respondents' privacy, and right to withdraw from my research at any time without any consequences for the respondents. I will use clear language and under no circumstances shall I force you to participate in my research.

The risk/s of the study are outlined as follows:

- There are no foreseeable risks in participating in the study.

BENEFITS OF THE RESEARCH

The Benefits of this research are outlined as follows:

- To contribute to information security research by developing an understanding of the importance of information security compliance in SMEs.

VOLUNTARY PARTICIPATION AND WITHDRAWAL

Your participation in this research is entirely voluntary, which means that you are free to decline participation. It is your decision whether or not to take part. If you volunteer to be in this study, you may withdraw at any time without consequences of any kind. If you decide to participate in the study, you are free to withdraw at any time – and without giving a reason. You may also choose not to

answer particular questions that are asked in the study. If there is anything that you would prefer not to discuss, please feel free to say so.



PAYMENT FOR PARTICIPATION

There are no costs to the participant for partaking in the study.

INFORMED CONSENT

Your signed consent to participate in this research study is required before you complete the questionnaire. I have included the consent form with this information sheet so that you will be able to review the consent form and then decide whether you would like to participate in this study or not.

QUESTIONS

Should you have further questions or wish to know more, I can be contacted as follows:

Student Name : Felencia Linthea Lawrence

Student Number : 3329196

Mobile Number : +27 65976 8709

Email : 3329196@myuwc.ac.za

I am accountable to my supervisor : Prof Osden Jokonya

Department : Information systems

Telephone : +27 21 959 1610

Fax : +27 21 959 3522

Email : ojokonya@uwc.ac.za

This research project has received ethical approval from the Humanities and Social Sciences Research Ethics Committee, Research Development, of the University of the Western Cape,
Tel. 021 959 2988,

Email: research-ethics@uwc.za



UNIVERSITY OF THE WESTERN CAPE
Faculty of Economic and Management Sciences
Department of Information Systems

APPENDIX C: Consent form for SMEs in Cape Town

RESEARCH TITLE: Factors affecting information security compliance among SMEs in Cape Town.

I have read the information presented in the information letter about a study being conducted by **Felencia Linthea Lawrence** for the Master's Programme at the Information Systems Department at the University of the Western Cape.

This study has been described to me in a language that I understand and I freely and voluntarily agree to participate. My questions about the study have been answered and I give my consent for any audio recording during this research project.

I understand that my identity will not be disclosed and was informed that I may withdraw my consent at any time by advising the student researcher.

With full knowledge of all the foregoing, I agree to participate in this study.

Participant Name : _____
Participant Signature : _____
Date : _____
Place : _____
Student Researcher : Felencia Linthea Lawrence
Student Researcher Signature : _____
Student Number : 3329196
Mobile Number : +27 65 976 8709
Email : 3329196@myuwc.ac.za



I am accountable to my supervisor : Prof Osden Jokonya
Department : Information Systems Department
Telephone : +27 21 959 1610
Fax : +27 21 959 3522
Email : ojokonya@uwc.ac.za

This research project has received ethical approval from the Humanities and Social Sciences Research Ethics Committee, Research Development, of the University of the Western Cape,
Tel. 021 959 2988,
Email: research-ethics@uwc.ac.za



UNIVERSITY OF THE WESTERN CAPE
Faculty of Economic and Management Sciences
Department of Information Systems

APPENDIX D: Information Security Survey for SMEs in Cape Town

You are invited to participate in an information security compliance survey conducted by Ms. Felencia Lawrence (Student number: 3329196). This survey is in partial completion of the researcher's thesis towards a Master's degree at the Department of Information Systems, at the University of the Western Cape. You are required to complete the personal and official information table below before you proceed to the conceptualization section.

PERSONAL AND OFFICIAL INFORMATION	
Biographical Details	Details
Company name:	
Name & Surname:	
Gender:	
Contact number:	
Email address:	
Position:	
Department:	
Length of time at the company:	



Instructions

Complete the survey by marking your preferred option with an X in the boxes provided. Only one choice is allowed.

TECHNOLOGICAL FACTORS IN SECURITY					
Statement	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
Technological Compatibility					
1. I know how to deal with information security accidents or breaches.					
2. I know how to use the current information security technology.					
3. I know the response procedures when an information security accident occurs.					
4. I intend to report any security break-ins of the organization's computers and network.					
5. I believe that the information I work with is adequately protected.					
6. I believe the business unit will survive if there is a disaster resulting in the loss of systems, people, and/or premises.					
Technological Complexity					
1. Information security compliance has affected my workload.					
2. I feel drained due to the information security policies in my organization.					



3. The security activities of my organization create many more requests, problems, or complaints in my job.					
4. I feel busy due to the security activities of my organization.					
5. I adapt my work practices to the information security policies and standards.					
6. I feel pressured due to the security activities of my organization.					

Existing Technology

1. The organization performs backup and restoration procedures on a regular basis and verifies that viruses are not corrupting the backup data.					
2. The organization encrypts its backup data storage devices.					
3. The employees can recognize a legitimate warning message from a scam message that could result in downloading a virus.					
4. Employees are informed of any formal incident management programs that are in place.					
5. The organization does perform a test data recovery from backups to verify integrity.					
6. I know the reporting procedure for losses from information security failure.					

ORGANIZATIONAL FACTORS IN SECURITY

Statement	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
-----------	----------------	-------	---------	----------	-------------------

Top Management Support

1. The organization provides training to help employees improve their awareness of computer and information security issues.					
--	--	--	--	--	--



2. The organization provides employees with education on computer software copyright law.					
3. The organization educates employees on their computer security responsibilities.					
4. In the organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use.					
5. The organization focuses more on managerial security than information security.					
6. Most employees know how to install and back-up information security applications or software.					

Information Security Awareness

1. I am careful not to discuss sensitive company information in public places.					
2. I do not leave sensitive data unattended in open areas (copiers, faxes, desktops).					
3. I understand what information is considered 'sensitive' (Confidential and Proprietary).					
4. I am familiar with the appropriate methods for transmitting, storing, labeling, and handling sensitive information.					
5. I always encrypt sensitive data when sending via external email and I know how/when hardware and mobile devices should be encrypted.					
6. My sensitive/critical data is backed up on a routine basis and data recovery is tested periodically.					

Organizational Learning Culture

1. I know what information security is.					
---	--	--	--	--	--



2. Information security is necessary for my department.					
3. The organization is committed to information security to protect information.					
4. I know what my responsibilities are regarding information security.					
5. I know of an information security breach within my business area within the last 12 months.					
6. I know my organization could be vulnerable to security breaches if I do not adhere to its information security policies.					

Policies and Standards

1. I am aware that the organization has a written information security policy.					
2. I know where to get a copy of the information security policy.					
3. I have read the information security policy.					
4. Information security policies are written in a manner that is clear and understandable.					
5. I understand the rules and regulations prescribed by the information security policies of my organization.					
6. The information security policies and standards implemented by the organization support the business strategy.					

ENVIRONMENTAL FACTORS IN SECURITY

Statement	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
-----------	----------------	-------	---------	----------	-------------------



Security Regulatory Concerns

1. I feel uncomfortable that my use of ICTs can be easily monitored for information security.					
2. I feel that my privacy can be compromised because my activities using ICTs can be traced to information security.					
3. I feel that my employer could violate my privacy by tracking my activities using ICTs for information security.					
4. I feel that my use of ICTs makes it easier to invade my privacy for information security.					
5. I feel that my personal information is violated through information security.					
6. I feel the use of ICTs to monitor my activities violates my privacy rights.					

Risks in Outsourcing

1. I know what is meant by information security outsourcing services and third-party tools.					
2. My organization utilizes the service of third parties to protect company data.					
3. I feel comfortable trusting a vendor with my work data.					
4. I trust that the tools provided by the vendor provide full protection against any security breaches.					
5. The software provided by the vendor is compatible with my digital skills.					
6. I am familiar with the technical prevention measures described by vendors.					



Security and Privacy Compliance

1. I fully understand the information security policies set out by my organization.					
2. I intend to comply with the requirements of the information security compliance of my organization in the future.					
3. I intend to protect company data by complying with the organization's information security policies.					
4. I intend to protect information and technology resources according to the requirements of the information security policies of my organization in the future.					
5. I intend to carry out my responsibilities prescribed in the information security policies of my organization when I use information and technology in the future.					
6. I consider anonymously reporting any non-compliant employees to top management.					

Thank you for your participation.



UNIVERSITY OF THE WESTERN CAPE
Faculty of Economic and Management Sciences
Department of Information Systems

APPENDIX E: Mean scores and Standard deviation

Descriptive Statistics					
	N	Min.	Max.	Mean	Std. Deviation
Technological Compatibility 1	120	1	5	3.54	.978
Technological Compatibility 2	120	1	5	3.72	.900
Technological Compatibility 3	120	1	5	3.64	.942
Technological Compatibility 4	120	1	5	3.34	.992
Technological Compatibility 5	120	1	5	2.18	.763
Technological Compatibility 6	120	1	5	3.83	.785
Existing Technology 1	120	1	5	4.35	.575
Existing Technology 2	120	1	5	4.34	.615
Existing Technology 3	120	1	5	4.28	.594
Existing Technology 4	120	1	5	4.07	.724
Existing Technology 5	120	1	5	3.34	1.141
Existing Technology 6	120	1	5	3.51	1.123
Technological Complexity 1	120	1	5	2.77	1.000
Technological Complexity 2	120	1	5	2.79	1.036
Technological Complexity 3	120	1	5	2.88	1.042
Technological Complexity 4	120	1	5	3.06	1.079
Technological Complexity 5	120	1	5	3.25	.955
Technological Complexity 6	120	1	5	2.97	1.073
Organizational Learning Culture 1	120	1	5	3.15	.941
Organizational Learning Culture 2	120	1	5	3.41	.884



Organizational Learning Culture 3	120	1	5	2.97	.978
Organizational Learning Culture 4	120	1	5	3.95	.659
Organizational Learning Culture 5	120	1	5	3.75	.713
Organizational Learning Culture 6	120	1	5	2.71	1.024
Information Security Culture 1	120	1	5	3.05	.960
Information Security Culture 2	120	1	5	3.10	1.016
Information Security Culture 3	120	1	5	3.29	.920
Information Security Culture 4	120	1	5	2.80	.984
Information Security Culture 5	120	1	5	2.83	.929
Information Security Culture 6	120	1	5	2.93	.968
Top Management Support 1	120	1	5	2.17	.560
Top Management Support 2	120	1	5	2.07	.413
Top Management Support 3	120	1	5	2.14	.490
Top Management Support 4	120	1	5	2.13	.477
Top Management Support 5	120	1	5	2.50	.889
Top Management Support 6	120	1	5	2.07	.433
Policies & Standards 1	120	1	5	3.30	.992
Policies & Standards 2	120	1	5	3.19	1.015
Policies & Standards 3	120	1	5	3.18	1.012
Policies & Standards 4	120	1	5	3.25	.964
Policies & Standards 5	120	1	5	3.24	.944
Policies & Standards 6	120	1	5	3.25	.955
Compliance 1	120	1	5	3.33	.936
Compliance 2	120	1	5	3.94	.626
Compliance 3	120	1	5	3.97	.634
Compliance 4	120	1	5	3.98	.608
Compliance 5	120	1	5	3.97	.586
Compliance 6	120	1	5	3.75	.843
Security Regulatory Concerns 1	120	1	5	2.64	.968
Security Regulatory Concerns 2	120	1	5	2.66	.992
Security Regulatory Concerns 3	120	1	5	2.69	1.035
Security Regulatory Concerns 4	120	1	5	2.66	1.000



Security Regulatory Concerns 5	120	1	5	2.65	1.026
Security Regulatory Concerns 6	120	1	5	2.65	1.026
Risk Of Outsourcing 1	120	1	5	3.63	.849
Risk Of Outsourcing 2	120	1	5	2.32	.926
Risk Of Outsourcing 3	120	1	5	2.45	.986
Risk Of Outsourcing 4	120	1	5	2.71	.911
Risk Of Outsourcing 5	120	1	5	2.68	.852
Risk Of Outsourcing 6	120	1	5	2.60	.883
Valid N (listwise)	120				

APPENDIX F: Plagiarism Similarity Index

preferences

previous paper next paper

Originality Report

Processed on: 31-Oct-2022 04:04 SAST
 ID: 1939754434
 Word Count: 41840
 Submitted: 1

last
 By Felencia Felencia

Similarity Index
23%

Similarity by Source

Internet Sources:	19%
Publications:	7%
Student Papers:	8%

Document Viewer

include quoted include bibliography exclude small matches

mode: show highest matches together



Factors affecting information security compliance among SMEs in Cape Town.
 Felencia Linthea Lawrence

A thesis submitted in fulfilment of the requirements for the degree of Master of Commerce in Information Systems in the Department of Information Systems Faculty of the Economic and Management Sciences University of the Western Cape Supervisor: Professor 3

Osdien Jokonya November 2022 PLAGIARISM DECLARATION Declaration I, Felencia Linthea Lawrence declare that "Factors affecting information security compliance among Small-medium enterprises (SMEs) in Cape town"

is my own work, that it has not been submitted for any degree or examination in any other university, and that all the sources I have used or quoted have been indicated and acknowledged by complete references. Full name: Felencia Linthea Lawrence Date: November 2022 Signature: _____ 135

- 1 1% match (Internet from 25-Nov-2020) ✖
<https://ajsel.aisnet.org/cgi/viewcontent.cgi?amp=&article=1021&context=acis2015>
- 2 1% match (Internet from 26-Dec-2021) ✖
<https://researchspace.auckland.ac.nz/bitstream/2021-thesis.pdf?isAllowed=y&sequence=1>
- 3 < 1% match () ✖
[Jacobs, Miriam. "The role of culture in mobile application adoption amongst diabetes patients in previously disadvantaged communities in the Western Cape", University of Western Cape, 2021](#)
- 4 < 1% match () ✖
[KWATSHA, NOLUTHANDO. "SMALL ENTERPRISE FINANCE AGENCY \(SEFA\). PREPAREDNESS TO IMPLEMENT THE PROTECTION OF PERSONAL INFORMATION \(PoPI\) ACT, No. 4 of 2013", 2020](#)
- 5 < 1% match () ✖