

A FRAMEWORK FOR END-USER COMPLIANCE WITH THE INFORMATION SECURITY
POLICY IN GOVERNMENT INSTITUTIONS

by

SAKHILE CHARITY DORIES LEKHULENI

submitted in accordance with the requirements for
the degree of

MASTER OF SCIENCE

In the subject

COMPUTING

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF ADÉLE DA VEIGA

2026

ABSTRACT

Employees' non-adherence causes most security breaches in both private and public organisations to information security policies (ISPs). The purpose of this research is to develop a framework for end-user compliance with ISPs in government departments. A framework that integrates all factors that enhance end-user compliance will assist organisations and information security managers in understanding the elements that affect end-user compliance. A systematic literature review was conducted using the PRISMA method to identify the factors and components contributing to the development of the framework. Moreover, semi-structured interviews were conducted with government officials from two Mpumalanga departments and with experts in information security and ISP compliance to refine and validate the framework. The outcome of the interviews with government officials and experts resulted in the inclusion of additional components and factors to the conceptual ECISP framework. The outcome of this process is a validated framework intended to enhance end-user compliance with ISPs within government institutions. The main aim of the research study is to integrate literature findings with practical insights from government officials and experts to develop, refine, and validate a framework for end-user compliance with ISPs in Government departments (the ECISP Framework). The ECISP Framework provides guidance that enables organisations to address specific challenges related to end-user compliance with ISPs, thereby improving the likelihood of achieving end-user compliance with ISPs.

Keywords: information security policy, end-user compliance with information security policy, government departments, ECISP Framework.

ACKNOWLEDGEMENTS

First and foremost, I give all glory and honour to the Lord Almighty for granting me the strength, wisdom, and perseverance to complete this research. His grace has sustained me throughout this journey, providing me with the faith and courage to keep moving forward. Without His grace, guidance, and provision, this journey would not have been possible.

My deepest gratitude goes to my supervisor, Prof. Adéle Da Veiga, for her invaluable guidance, support, and mentorship throughout this study. Your encouragement, patience, and constructive feedback have shaped not only this work but also my academic growth.

To my husband, thank you for your unwavering support, encouragement, and belief in me. You have been my rock and my number one supporter alongside my mother, carrying me through the challenges of this journey.

To my mother, Salaphi Lekhuleni, my cheerleader and prayer warrior, I owe my deepest thanks. Words cannot express my gratitude. Your unwavering prayers, encouragement, and faith in me have carried me through the most challenging times.

To my beloved children, Sinesipho, Siyanda, and Zanoxolo, thank you for your love, patience, and understanding when my studies took up much of the time I should have spent with you. Your support has been my greatest motivation to press on.

I also extend special thanks to my cousin and sister, Fikile Ngomane, who has always been the voice of reason during difficult times. Thank you for reminding me of my capabilities, encouraging me to believe in myself, and pushing me never to give up when challenges arise.

Finally, I am grateful to my family and friends for their encouragement and support throughout this academic endeavour.

The financial assistance provided by the University of South Africa (UNISA) towards this research is hereby acknowledged with appreciation. The opinions expressed and the conclusions arrived at are those of the author and should not be attributed to UNISA.

DECLARATION

I Sakhile Charity Dorries Lekhuleni, hereby declare that this document: **A FRAMEWORK FOR END-USER COMPLIANCE WITH THE INFORMATION SECURITY POLICY IN GOVERNMENT INSTITUTIONS**, submitted for evaluation towards the requirements for completed a Master of Science in Computing qualification at the University of South Africa, is my own original work and has not been previously submitted to other institutions of higher learning or subject for evaluation. All sources used or quoted in this document are indicated and acknowledged by means of a list of references.

Surname, Initials: Lekhuleni SCD

Student No: 34906592

Signature 

Date 19/07/2026

Table of contents

GLOSSARY OF TERMS	11
LIST OF ACRONYMS	11
1. CHAPTER 1 INTRODUCTION	13
1.1 OVERVIEW OF CHAPTER 1	14
1.2 BACKGROUND	14
1.3 PROBLEM STATEMENT AND RESEARCH OBJECTIVES	16
1.3.1 MAIN RESEARCH QUESTION.....	17
1.3.2 SUB RESEARCH QUESTIONS.....	17
1.3.3 RESEARCH OBJECTIVES	18
1.3.4 RESEARCH APPROACH & METHOD.....	19
1.4 SCOPE OF THE STUDY	23
1.5 CONTRIBUTIONS OF THE STUDY.....	23
1.6 LIMITATIONS.....	23
1.7 ETHICAL CONSIDERATIONS	24
1.8 CHAPTER OUTLINE	24
1.9 SUMMARY	25
2. CHAPTER 2: LITERATURE REVIEW	27
2.1 INTRODUCTION	27
2.2 OVERVIEW OF CHAPTER 2	28
2.3 SCOPING LITERATURE REVIEW.....	28
2.3.1 OVERVIEW OF SCOPING LITERATURE REVIEW	28
2.3.2 IDEAL REPORTING ITEMS FOR SYSTEMATIC REVIEWS AND META-ANALYSIS (PRISMA) METHOD	28
2.3.3 LITERATURE SOURCES.....	29
2.3.4 INCLUSION AND EXCLUSION CRITERIA	29
2.3.5 LITERATURE SEARCH, SCREENING, ANALYSIS AND SELECTION	31
2.4 INFORMATION SECURITY POLICY	33
2.4.1 DEFINING INFORMATION SECURITY POLICY	33
2.5 END-USER COMPLIANCE WITH INFORMATION SECURITY POLICIES	34
2.5.1 DEFINING END-USER COMPLIANCE TO INFORMATION SECURITY POLICIES ..	34
2.5.2 THE IMPORTANCE OF END-USER COMPLIANCE TO INFORMATION SECURITY POLICIES	35

2.6	OTHER RESEARCHERS' APPROACHES TO IMPROVE END-USER COMPLIANCE WITH INFORMATION SECURITY POLICIES	36
2.6.1	GEOGRAPHY.....	36
2.6.2	ENVIRONMENT	37
2.6.3	FRAMEWORK DEVELOPMENT AND VALIDATION.....	37
2.6.4	THEORIES USED	37
2.6.5	FACTORS USED/IDENTIFIED	39
2.7	SUMMARY	45
3.	CHAPTER 3 THE CONCEPTUAL FRAMEWORK	46
3.1	INTRODUCTION	46
3.2	THE CONCEPTUAL ECISP FRAMEWORK DEVELOPMENT APPROACH.....	47
3.3	DEFINING A CONCEPTUAL FRAMEWORK.....	47
3.4	COMPONENTS OF THE FRAMEWORK	47
3.4.1	THEORY OF PLANNED BEHAVIOUR	49
3.4.2	ETHICS.....	50
3.4.3	BEHAVIOURAL MOTIVATORS	51
3.4.4	SECURITY EDUCATION, TRAINING AND AWARENESS (SETA).....	53
3.4.5	LEADERSHIP, MANAGEMENT AND GOVERNANCE.....	54
3.5	THE CONCEPTUAL ECISP FRAMEWORK	55
3.5.1	THE APPROACH TO CONCEPTUAL FRAMEWORK DEVELOPMENT.....	55
3.5.2	ILLUSTRATING THE CONCEPTUAL ECISP FRAMEWORK.....	56
3.6	SUMMARY	58
4.	CHAPTER 4: RESEARCH METHODOLOGY	59
4.2	RESEARCH DESIGN PROCESS	60
4.2.1	RESEARCH PHILOSOPHY	61
4.2.2	RESEARCH APPROACH	64
4.2.4	DATA COLLECTION TECHNIQUES	73
4.2.5	SAMPLE SELECTION	76
4.2.6	DATA COLLECTION	79
4.2.7	DATA ANALYSIS	79
4.2.8	DATA VALIDITY AND RELIABILITY	80
4.2.9	INTERVIEW BIAS.....	81

4.3	INTERVIEW GUIDE.....	81
4.3.1	INTERVIEW GUIDE FOR GOVERNMENT OFFICIALS – REFINEMENT.....	81
4.4.	LIMITATIONS	83
4.6	SUMMARY	84
5.	CHAPTER 5: REFINEMENT AND VALIDATION OF THE PROPOSED ECISP FRAMEWORK.....	85
5.1	INTRODUCTION.....	85
5.2	OVERVIEW OF CHAPTER 5	86
5.2.1	STAGES OF REFINING AND VALIDATING THE FRAMEWORK	86
5.3	FRAMEWORK REFINEMENT AND VALIDATION: APPLYING YIN’S CASE STUDY METHOD	87
5.3.1	FRAMEWORK REFINEMENT	87
5.3.2	FRAMEWORK VALIDATION	102
5.4	SUMMARY	120
6.	CHAPTER 6: CONCLUSION	122
6.1	INTRODUCTION.....	122
6.2	OVERVIEW OF CHAPTER 6	123
6.3	REVIEW OF THE RESEARCH PROBLEM	123
6.4	REFLECTION ON RESEARCH QUESTIONS	124
6.5	SUMMARY OF THE RESEARCH DESIGN	127
6.6	SUMMARY OF RESEARCH CHAPTERS	128
6.7	RESEARCH CONTRIBUTIONS.....	129
6.8	LIMITATIONS	130
6.9	FUTURE RESEARCH	130
6.10	CONCLUSION.....	131
7.	REFERENCES.....	132
8.	LIST OF APPENDICES.....	149
8.1	APPENDIX A: LIST OF FACTORS.....	149
8.3	APPENDIX B: ETHICS APPROVAL	177
8.4	APPENDIX C: PERMISSION LETTERS.....	179
8.5	APPENDIX D: CONSENT FORMS	181
8.6	APPENDIX E: INTERVIEW GUIDE -GOVERNMENT OFFICIALS	182
8.7	APPENDIX F: INTERVIEW GUIDE-EXPERTS.....	185

8.8	APPENDIX G: EMAIL INVITATION	188
8.9	APPENDIX H: PUBLISHED CONFERENCE PAPER.....	189
8.10	APPENDIX I: LANGUAGE EDITITING CERTIFICATE	202

LIST OF TABLES

<i>Table 1-1: Research Questions</i>	19
<i>Table 2-1: Summary of the Search Criteria</i>	30
<i>Table 2-2 : Theories used in Studies</i>	37
<i>Table 2-3: List of Factors per Category</i>	39
<i>Table 3-1: Factors Related to the Theory of Planned Behaviour</i>	50
<i>Table 3-2: Factors Related to Ethics</i>	51
<i>Table 3-3: Behavioural Related Factors</i>	52
<i>Table 3-4: SETA Related Factors</i>	54
<i>Table 3-5: Leadership, Management and Governance</i>	55
<i>Table 4-1: Interpretivist Assumptions: Adapted from (Cresswell 2009)</i>	63
<i>Table 4-2: Characteristics of Inductive, Deductive and Abductive Approaches, adapted from Saunders et al. 2015; and Saunders 2023</i>	64
<i>Table 4-3: Characteristics of Qualitative Research</i>	66
<i>Table 4-4: Characteristics of Research Strategies, adapted from Cresswell (2007)</i>	68
<i>Table 4-5: Frequently Used Data Collection Instruments</i>	74
<i>Table 4-6: Government Officials' Roles and Years of Experience</i>	76
<i>Table 4-7: Experts' Knowledge Domain and Years of Experience</i>	77
<i>Table 5-1: Stages of Refining and Validating the Framework</i>	86
<i>Table 5-2: Explanation of Factors</i>	116

LIST OF FIGURES

<i>Figure 1-1: Phases of the Study</i>	<i>22</i>
<i>Figure 2-1: Prisma Diagram: Prisma Diagram of Scoping Literature Review</i>	<i>32</i>
<i>Figure 3-1: The Five Components of the Framework.....</i>	<i>48</i>
<i>Figure 3-2: The Conceptual Framework</i>	<i>57</i>
<i>Figure 4-1: Research Onion.....</i>	<i>60</i>
<i>Figure 4-2: Phases of the Study, adapted from Yin (2003)</i>	<i>70</i>
<i>Figure 5-1: Completeness of the Framework - Thematic Diagram</i>	<i>88</i>
<i>Figure 5-2: Suitability of the Framework - Thematic Network Diagram</i>	<i>90</i>
<i>Figure 5-3: Applicability of the Framework - Thematic Network Diagram</i>	<i>92</i>
<i>Figure 5-4: Usability of the Framework - Thematic Network Diagram</i>	<i>94</i>
<i>Figure 5-5: Most Suitable and Relevant Components and Factors - Thematic Network Diagram</i>	<i>96</i>
<i>Figure 5-6: Proposed New Components and Factors - Thematic Network Diagram.....</i>	<i>98</i>
<i>Figure 5-7: The Refined Framework</i>	<i>101</i>
<i>Figure 5-8: Framework Accuracy - Thematic Network Diagram.....</i>	<i>103</i>
<i>Figure 5-9: Framework Comprehensiveness - Thematic Network Diagram.....</i>	<i>104</i>
<i>Figure 5-10: Framework Relevancy - Thematic Network Diagram</i>	<i>105</i>
<i>Figure 5-11: Framework Effectiveness - Thematic Network Diagram.....</i>	<i>106</i>
<i>Figure 5-12: Most Contributing Components - Thematic Network Diagram.....</i>	<i>107</i>
<i>Figure 5-13: Proposed Additional Components - Thematic Network Diagram</i>	<i>108</i>
<i>Figure 5-14: Proposed Additional Factors - Thematic Network Diagram</i>	<i>109</i>
<i>Figure 5-15: Proposed Framework Adjustments - Thematic Network Diagram.....</i>	<i>111</i>
<i>Figure 5-16: Potential Challenges and Limitations - Thematic Network Diagram</i>	<i>112</i>
<i>Figure 5-17: Validated Framework/ ECISP Framework.....</i>	<i>115</i>

GLOSSARY OF TERMS

TERM	DEFINITION
Conceptual Framework	A model that identifies and illustrates the key concepts and relationships relevant to a study (Demissew et al., 2015).
Conceptual ECISP Framework	In the context of this study, a conceptual End-user Compliance with Information Security Policy (ECISP) framework developed in this study based on literature review to enhance end-user compliance to ISP in government departments.
ECISP Framework	In the context of this study, a framework developed in this study to enhance end user compliance to ISP in government departments.
End-user	Refers to employees who use the organization's information systems, application or technology to perform their tasks (Au, Ngai, and Cheng, 2002).
End-user Compliance with ISP	End-user compliance with the ISP refers to the extent to which end-users comply with the organisation's prescribed information security rules, procedures, and core security activities as outlined in the ISP (Baloizian & Leidner, 2017; Julisch, 2008; Balagopal & Mathew, 2024; Padayachee, 2012).
Information Security	The protection of information from unauthorized access, disclosure, alteration, disruption, or destruction (Nieles et al., 2017).
Information Security Policy	A formal set of rules, guidelines, and procedures that govern the protection and use of an organization's information assets (Alzahrani, 2021; Baloizian & Leidner, 2017; Corpuz, 2011; Kabanda & Mogoane, 2022).
Insider Threat	A security risk that is realised as a result of employees within an organization intentionally or unintentionally compromising information security (Nurse et al., 2014).
Qualitative Research	A research approach that involves interpreting data to understand the meanings individuals ascribe to it and the methods used to generate it for analysis (Creswell, 2007; Creswell & Poth, 2016; Kennedy, 2019; Quinn Patton & Cochran, 2007).
Refined ECISP Framework	In the context of this study, Refined ECISP Framework refers to a framework developed in this study based on the literature review and improved through interviews with government officials to enhance end-user compliance with ISP.
Semi-Structured Interviews	An interview method that uses open-ended set of predefined questions while allowing participants to response to be explorative while allowing the interviewer to ask follow-up questions (Magaldi & Berler, 2020).
Thematic Analysis	A method of identifying, analysing, and reporting patterns or themes within qualitative data (Braun & Clarke, 2006).
Validated ECISP Framework	In the context of this study, Validated ECISP Framework refers to a framework developed in this study through literature review and improved through interviews with experts to enhance end-user compliance with ISP

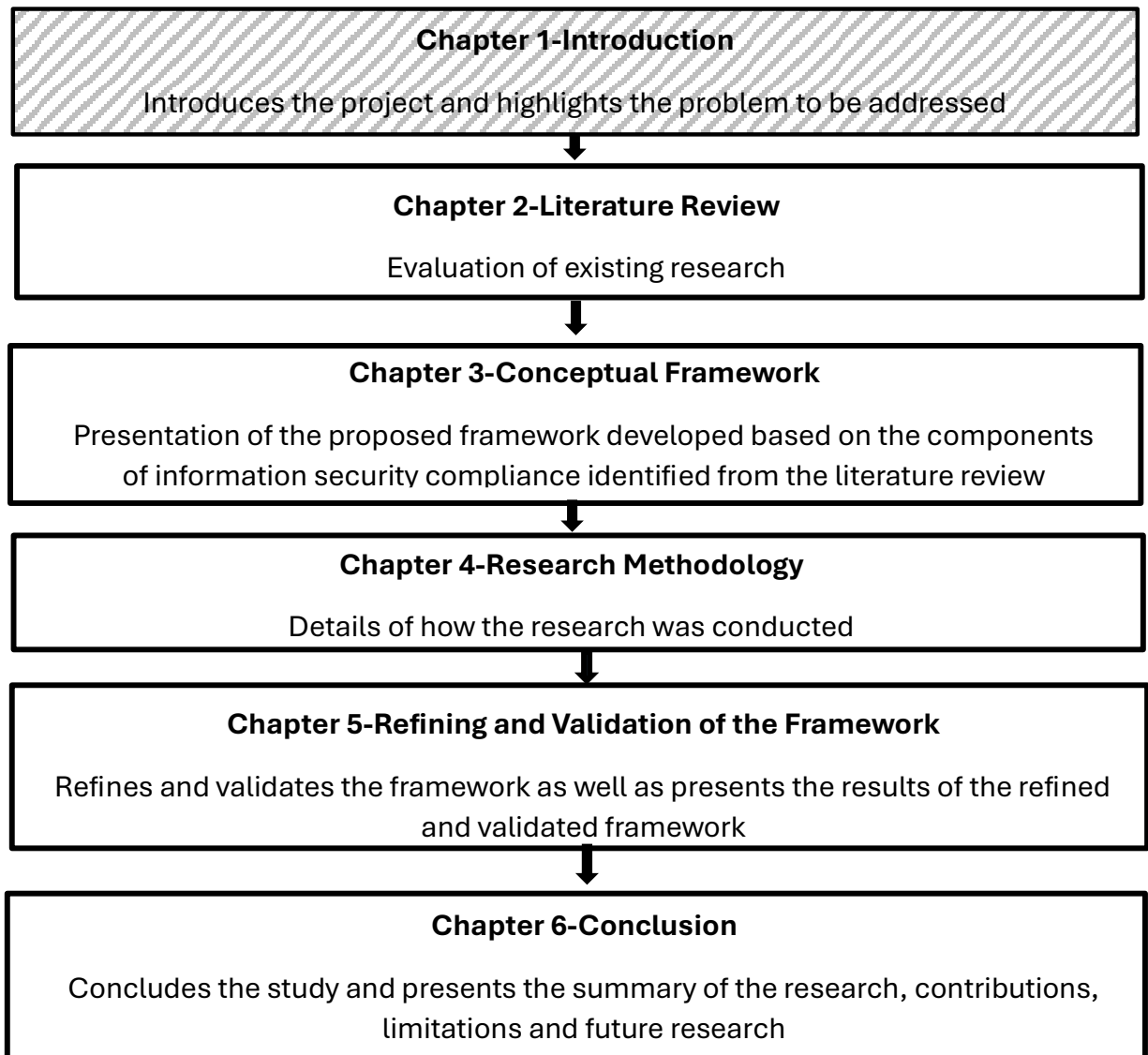
LIST OF ACRONYMS

ACRONYM	DEFINITION
ECISP	End-user Compliance with Information Security Policy
SETA	Security Training, Education and Awareness
ISP	Information Security Policy

PUBLICATIONS

Lekhuleni, S. C. D., & Da Veiga, A. (2025). End-User Compliance with Information Security Policy Framework for Government Departments in South Africa. *International Conference on Advanced Research in Technologies, Information, Innovation and Sustainability, ARTIIS 2024. Communications in Computer and Information Science*, 2347(March), 283–300.
<https://doi.org/10.1007/978-3-031-84078-4>

1. CHAPTER 1 INTRODUCTION



1.1 OVERVIEW OF CHAPTER 1

The study examines the causes of non-compliance. It also compiles a list of factors that contribute to compliance with organisations' information security policies (ISPs). It then develops a framework to enhance end-user compliance with information security policies within a South African government department, that has existing ISPs.

This chapter provides an overview of the work described in this dissertation. The chapter is structured as follows: section 1.2 outlines the background to the study; section 1.3 presents the problem statement, the research objectives, the research question and the aim; section 1.4 summarises the research methodology used in this study; section 1.5 reflects on the scope of the study; section 1.6 discusses the contributions of the study; section 1.7 discusses the ethical considerations; and section 1.8 outlines the layout of the dissertation.

1.2 BACKGROUND

Information leakage and policy violations have been experienced by several organisations due to the increase in cyber-attacks and the lack of structured mechanisms for policy compliance and enforcement (Mandal, 2021; Smita Verma, 2025; Wu et al., 2012). Most security breaches in organisations are caused by employees' non-adherence to security policies (Alzahrani, 2021; Beautelement et al., 2008). ISP compliance is when employees comply with an ISP's requirements to protect the organisation's information technology resources. Information security compliance is also defined as conformance with compulsory security procedures and standards (Julisch, 2008).

Organisations use ISPs as guidelines for acceptable employee behaviour. Organisations depend on ISPs as guidelines for end-user acceptable behaviour towards protecting the organisation's information. Nonetheless, end-user compliance with information security policies is still a challenge and violations of these policies are very common (Ali, et al., 2021; Alotaibi et al., 2016; Liu et al., 2020; Sohrabi Safa et al., 2016; Vadisetty, 2024). Employees are regarded as the most significant contributing factor in these violations (Aurigemma & Panko, 2012; Liu et al., 2020a; Mani et al., 2015; Simon, 2014; Tsohou et al., 2015; Vadisetty, 2024).

Insider threats and non-compliance with the ISP have been recognised as one of the major challenges organisations face (Alotaibi et al., 2016; Saxena et al., 2020; Willison & Warkentin, 2013). Sherif et al. (2015) found that 35% of global data breaches are caused by human error. A

report by PricewaterhouseCoopers (2018) states that incidents attributed to insiders, comprising suppliers, consultants, contractors and employees, contributed 30% of the incidents reported in 2017. In addition, according to Ponemon Institute's (2022) global report, insider threats rose by 44% since 2020, and the average annual cost was \$15.4 million. Furthermore, the report indicates that 56% of incidents were due to negligence, and the average cost was \$ 6.6 million per year (Ponemon Institute, 2022). Moreover, according to a report by Cybersecurity Insiders, 83% of organisations reported at least one insider attack in 2024 (Cyber Security Insiders:2024 Insider Threat Report, 2024).

To address this challenge, organisations should transform users from an information security vulnerability into the first line of defence for ISP compliance by implementing a people-centric insider threat management programme (Ng et al., 2009; Ponemon Institute, 2022). Implementing the right technology does not guarantee that information is properly secured (Alzahrani, 2021; Cannoy & Salam, 2010; Hossain et al., 2025). Researchers (Kirlappos et al., 2015a; Balagopal & Mathew, 2024; Ponemon Institute, 2022), suggest that security managers should include compliance and human behaviour within the organisation's security management procedures. Employees who adhere to the information security guidelines and principles are crucial to reinforcing effective information security management (Arcy & Teh, 2019; Bulgurcu et al., 2009; Hossain et al., 2025). Similarly, employees who do not adhere to security policy requirements are among the main threats to organisations determined to safeguard their information technology systems and information (Beris et al., 2015; Liu et al., 2020).

Several studies have examined ISP compliance (Alzahrani, 2021; Balagopal & Mathew, 2024; Yazdanmehr & Wang, 2016). However, the focus has been on identifying the factors that influence employee compliance and non-compliance with the ISP (Delso-Vicente et al., 2025; Safa et al., 2015; Shih & Liou, 2015; Topa & Karyda, 2015). A study that consolidates all factors to develop a framework for information security compliance has not been found. A consolidated framework that incorporates all relevant factors will help organisations and security managers understand the factors affecting information security compliance and, in turn, improve end-user compliance by implementing the ECISP framework and leveraging on the identified factors and components of the ECISP framework.

1.3 PROBLEM STATEMENT AND RESEARCH OBJECTIVES

Information security is a key factor affecting organisations. According to various authors, information security is a challenge in organisations (Ahmed & Abas, 2024; Alassaf & Alkhalifah, 2021; Safa et al., 2015). Human factors have been identified as key source of information security risks in organisations (Assefa & Tensaye, 2021; Delso-Vicente et al., 2025). While advanced technologies have improved efficiency in, it also introduces information security risks, such as creating opportunity for hackers and cybercriminals, system failures, and data quality risks (Safa et al., 2016). Organisations have developed good ISPs, but employee compliance remains a challenge (Hossain et al., 2025; Topa & Karyda, 2015). Failure to comply with ISP by employees exposes organizations to security risks, such as; data breaches, financial losses, operational disruption, and reputational damage (Caryn, 2021; Hamid & Huda, 2025; Toyana, 2021).

Several researchers have conducted studies on information security compliance (Ahmed & Abas, 2024; Aurigemma & Panko, 2012; Beris et al., 2015; Bulgurcu et al., 2010; Delso-Vicente et al., 2025). The focus of research studies associated with ISP compliance has predominantly been on identifying the factors that affect employees' non-compliance and compliance with the ISP (Delso-Vicente et al., 2025; Safa et al., 2015; Shih & Liou, 2015; Topa & Karyda, 2015).

Most research on ISP compliance has focused on the banking and health sectors; few studies have examined ISP compliance in the government sector. Government institutions are also experiencing data breaches that result in the loss of critical information and resources, causing economic damage (Caryn, 2021; Hamid & Huda, 2025; Toyana, 2021). Furthermore, online criminals are increasingly targeting some of South Africa's most crucial government departments (Caryn, 2021). Most attackers use ransomware, which is usually distributed via phishing emails or by utilising compromised user authorisation details (Rick Crouch & Associates private investigators, 2021). These types of attacks require end-user action to be successful; if end-user compliance is not instilled in government departments, loss of data, cyber-attacks and system disruption will remain challenge within the government environment. End-user compliance with the ISP can help improve end-user behaviour and reduce data breaches in organisations.

In addition, most studies focus on identifying the factors that enhance end-user compliance without developing a framework. The focus of these studies is on analysing the causes of non-compliance. The analysis provides an overview of the causes of non-compliance but does not offer guidelines

for improving information security compliance in organisations. A framework that consolidates and validates all factors that enhance information security compliance in the South African government has not been found.

1.3.1 MAIN RESEARCH QUESTION

The main research question of this study is:

What elements constitute a framework for end-user ISP compliance within a government institution in South Africa?

1.3.2 SUB RESEARCH QUESTIONS

SRQ1: What does existing research reveal about the current state and factors affecting end-user compliance with ISP?

Rationale: This sub-research question focuses on understanding the current state of ISP compliance and the factors that affect end-user compliance as identified by other researchers.

Understanding the current state of ISP compliance helps the researcher identify gaps which will in turn help to propose a suitable framework for improving information security compliance in organisations.

SRQ2: How can the existing literature help constitute a conceptual framework for end-user compliance with the ISP?

Rationale: This sub-research question focuses on how information from existing literature will be used to develop a conceptual framework. Information from the existing literature was used to identify components and factors used to develop the conceptual framework.

SRQ3: What elements constitute a validated framework for end-user ISP compliance within a government institution in South Africa?

Rationale: This sub-research focuses on identifying the components and factors that will be used to formulate a validated framework. The conceptual framework was refined and validated through interviews with government officials and experts, respectively, to update the conceptual framework that was developed from the literature review.

1.3.3 RESEARCH OBJECTIVES

The key objective of this study is to propose a framework to enhance end-user compliance with the ISP in South African government institutions.

To achieve the study's intended purpose, the following objectives were identified:

- To develop a framework for end-user compliance with the ISP.
- To review relevant literature to identify factors and components of the proposed framework.
- To develop the conceptual framework using the identified components.
- To validate the conceptual framework to ensure applicability, usability and suitability in a government institution in South Africa.

Table 1-1 provides a summary of the research questions and related research objectives. The table includes, in column three, the related chapter and deliverables for each phase of the study.

Table 1-1 Research Questions

Research Questions	Objectives	CHAPTER	DELIVERABLE
Main: What elements constitute a framework for end-user ISP compliance within a government institution in South Africa?	To develop a framework for end-user compliance with the ISP in South African government institutions.	Chapter 5 Refinement and validation of the ECISP Framework.	Refined and validated ECISP Framework.
SRQ1: What does existing research reveal about the current state and factors affecting end-user compliance with ISP?	To review relevant literature to identify factors and components for the proposed framework.	Chapter 2 Literature review.	Literature review. Components for the conceptual framework.
SRQ2: How can the existing literature help constitute a conceptual framework for end-user compliance with ISP?	To develop the conceptual framework using the identified components.	Chapter 3 The conceptual framework.	Conceptual ECISP Framework.
SRQ3: What elements constitute a validated framework for end-user ISP compliance within a government institution in South Africa?	To validate the conceptual framework to ensure applicability, usability and suitability within a government institution in South Africa.	Chapter 4 Research Methodology. Chapter 5 Validation and assessment of the ECISP Framework.	Validated ECISP Framework.

1.3.4 RESEARCH APPROACH & METHOD

This section discusses a short summary of the research approach and method to outline the key research phases in Fig 1-1 as a roadmap for the dissertation. A full discussion of the research methodology is presented in Chapter 4.

The study is grounded in an interpretivist research philosophy, using abductive reasoning (Creswell, 2014). It is implemented through a qualitative research approach using a case study design (Yin, 2003). Interpretivists argue that knowledge is subjective and that, to comprehend human action, the world should be seen through the eyes of the actors performing it. Interpretivism focuses on understanding human experiences, perceptions, and social context to construct reality (Alharahsheh & Pius, 2020). Interpretivism approaches research in a qualitative manner, using techniques such as unstructured interviews or participant observation. This philosophy is considered suitable for this research for the following reasons:

- The study focuses on the development of a framework that will assist organisations to improve employee compliance, i.e., human behaviour.
- The development of the framework involves understanding participants' points of view (Ryan, 2018). In this case, the interviews with government officials and the expert interviews.

The study was conducted in three phases; each phase informed the next. The three phases were adopted from the Yin case study method (Yin, 2003). Yin describes the case study research method as an iterative process in which each phase is linked to the others. Furthermore, each phase requires the researcher to review former decisions.

Phase 1: Define and design

Yin (2003) describes this phase as the process of identifying the theory to be examined in the case study. This phase of the literature review outlines the factors that enhance end-user compliance with the information security policy.

Phase 2: Prepare, collect, and analyse

This phase outlines the preparation for data collection, the principles of data collection, and the data analysis strategy. In this study, this phase entails developing the conceptual ECISP Framework using the components identified in Chapter 3. The framework is refined by government officials in information security and validated by information security experts through interviews. The refinement and validation aim to assess and confirm the framework's suitability, usability, completeness, and applicability within government institutions in South Africa.

Interviews were conducted with participants from two government departments and with information security experts. For government officials, interview questions were developed based on pre-defined themes derived from the proposed conceptual ECISP Framework. The questions were shared with government officials in advance of the interview to allow adequate preparation. These interviews with government officials were used to collect qualitative data on their views and to assess the proposed framework's suitability and usefulness within a government department. The results from these interviews were used to refine the conceptual ECISP Framework.

For the expert review, interviews were conducted with professionals in information security and ISP compliance. The interview questions, also derived from the proposed framework, were shared with experts in advance to allow adequate preparation. The purpose of the expert interviews was to assess the accuracy, comprehensiveness, relevance, and effectiveness of the refined framework. The results of the expert interviews were used to validate the refined framework.

A purposive sample of government officials and information security experts was selected, and interviews were conducted online. All interview data were transcribed and analysed using Atlas.ti.

The insights obtained from both the refinement (government officials) and validation (experts) phases were used to enhance and finalise the framework.

Phase 3: Recommendation and Conclusion

This phase presents the final framework, namely the ECISP Framework, to enhance end-user compliance in South African government institutions. It also provides conclusions and recommendations regarding areas of concern that could hinder effective application of the framework to improve end-user compliance with the ISP in South African government institutions.

The three phases are illustrated in **Figure 1-1**. The figure outlines which chapters fall within each phase of the study. For each chapter, the focus, research approach and final deliverable are depicted.

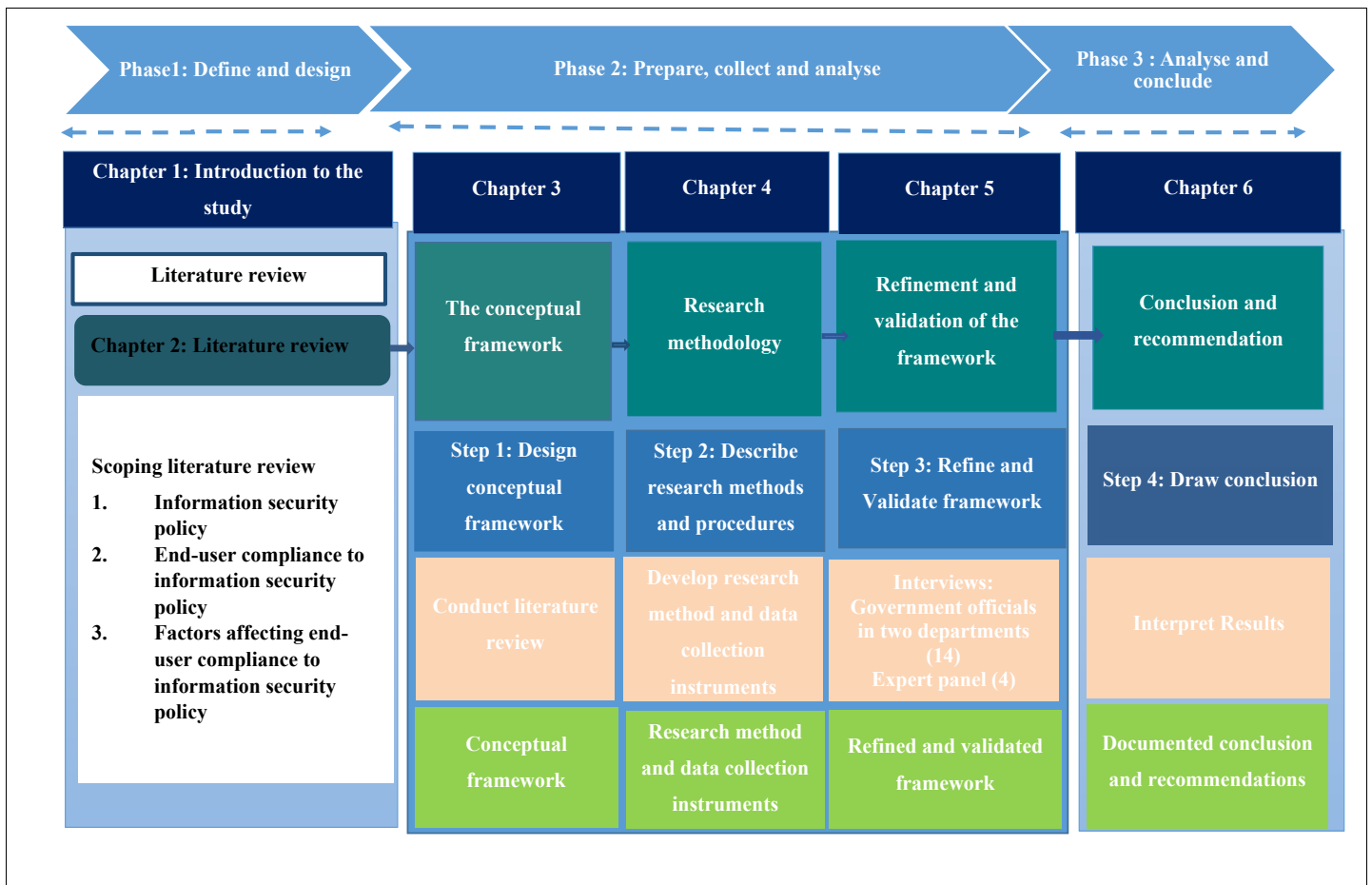


Figure 1-1: Phases of the Study

1.4 SCOPE OF THE STUDY

The study aims to develop a framework that integrates factors and components from the literature and government perspectives to support a South African government department in improving end-user ISP compliance. The concept, end user ISP, could include more than one policy relevant to information security compliance, such as the information security policy, end user computing policy, privacy policy, and other related information security policies.

1.5 CONTRIBUTIONS OF THE STUDY

The study aims to develop a framework to improve end-user ISP compliance in government institutions. The framework can serve as a guide to cultivate compliance with the ISP in government departments in South Africa. The study contributes by consolidating the components and factors identified through a systematic literature review and by providing a comprehensive framework for enhancing end-user ISP compliance. Furthermore, the framework is grounded in the South African government context and has been refined and validated through input from government officials and information security experts. This ensures that the framework is contextually relevant, implementable, and that it can effectively guide the adoption of ISP compliance practices within South African government institutions.

1.6 LIMITATIONS

The framework was refined in two government institutions, and experts were consulted for validation. Therefore, the information provided may be limited to the two departments and their respective areas of expertise. The results may not reflect a holistic view of the subject matter.

1.7 ETHICAL CONSIDERATIONS

The ethical aspects were considered to ensure that participants' rights were protected. Ethical issues were addressed during and after the research. Ethical clearance was obtained from the School of Computing Research Ethical Clearance Committee at UNISA, under certificate **reference number 2036**.

The research incorporated the following ethical requirements:

- The participants were informed of the study's purpose, and participation was voluntary.
- Confidentiality of information and the anonymity of the participants were ensured.
- The rights of participants were sent to the participants, and they were requested to confirm that they understand their rights before initiating any participation.

1.8 CHAPTER OUTLINE

This study comprises six chapters, organised as follows:

Chapter 1 - Introduction

Introduces the research and highlights the problem to be addressed.

Chapter 2 - Literature Review

Evaluation of existing research to gain insight into the research field, provide an overview of end-user compliance research with the ISP, identify research gaps, and motivate the need for this research. Identification of existing factors and components that enhance compliance, as well as components of the conceptual ECISP Framework based on the literature.

Chapter 3 - The conceptual framework for end-user compliance with the ISP within a government department.

Development of the proposed framework using the identified components.

Chapter 4 – Research Methodology

This chapter explains how the research was conducted, including a discussion of the method used, namely, a qualitative approach.

Chapter 5 – Refinement and Validation of the Framework

Refining and validating the framework and presenting the refined and final validated ECISP Framework.

Chapter 6 - Conclusion

Concludes the study and presents a summary of the research, contributions, limitations and future research.

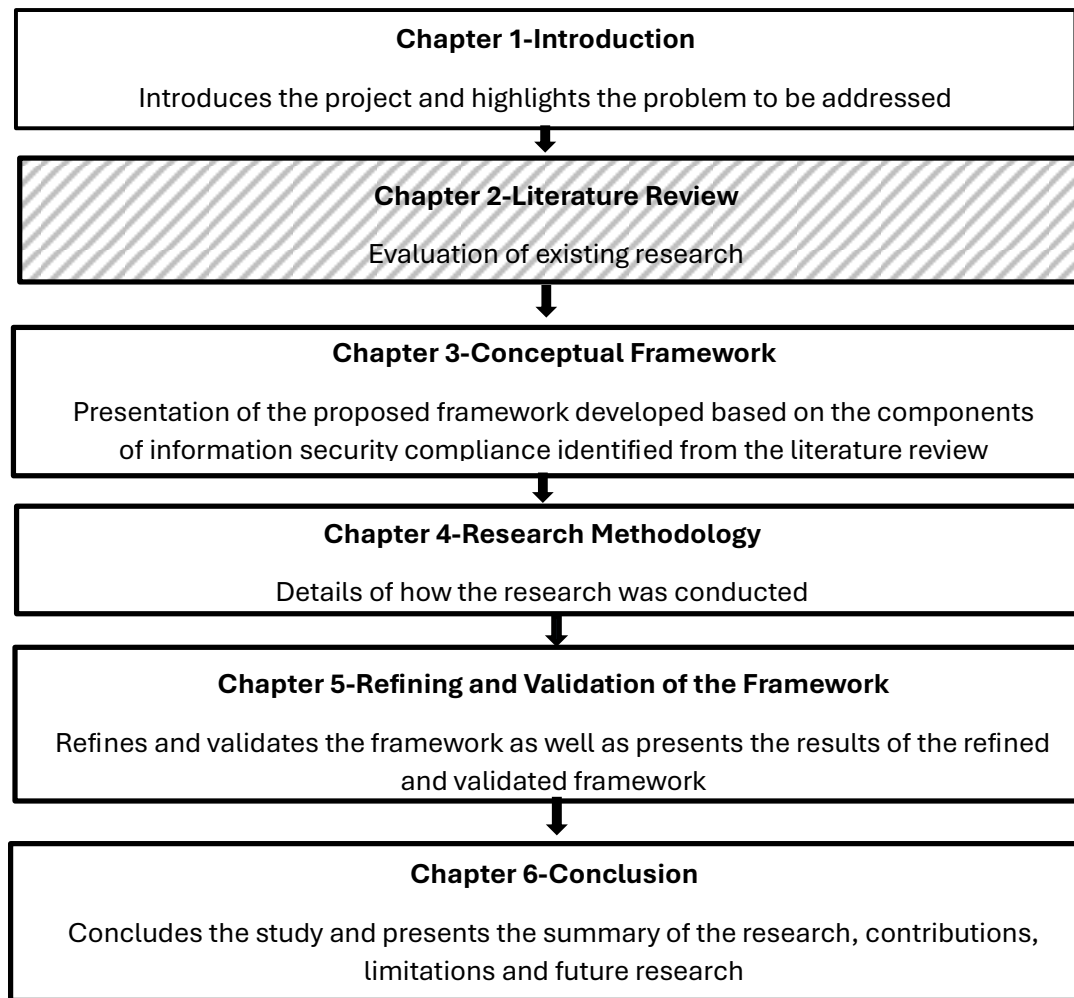
Appendices: This research report consists of appendices attached at the end of the report showing the additional material that was used in this study. **APPENDIX A** presents the list of factors identified through the literature review, outlined in a table that consists of a list of studies assessed, theories used by the studies, identified factors, studies that developed frameworks, studies that validated frameworks, studies conducted in Government and studies conducted in South Africa. **APPENDIX B:** presents the ethical clearance approval that was obtained for the study. **APPENDIX C** Presents the permission letters obtained from the two government departments to interview their officials. **APPENDIX D** and **APPENDIX E** presents the consent forms that were sent to government officials and experts to ensure voluntary participation and consent. **APPENDIX F** presents the interview guide that was sent to participants and used for the interview. **APPENDIX G** consists of the email invitation that was sent to participants inviting them to participate in the study. **APPENDIX H** presents the conference paper that was developed and published based on the study. **APPENDIX I** presents the language editing certificate that confirms that the research report was edited.

1.9 SUMMARY

This chapter presented the research outline, which is developed in the succeeding chapters. It outlined the study's aims, including the research questions. A brief overview of the research methodology and the study's scope was provided. The study's contribution and prominence were outlined, and high-level ethical considerations were specified.

Chapter 2 presents a literature review, adopting a scoping approach to examine the concept of ISP compliance and relevant behavioural theories. Additionally, it seeks to identify the factors that affect end-user compliance with the ISP.

2. CHAPTER 2: LITERATURE REVIEW



2.1 INTRODUCTION

Chapter 1 provides the background of the research, together with a description of the research problem in relation to the research objectives and questions. Chapter 2 provides an overview of ISP compliance. It defines what an ISP is, what end-user compliance entails, and why it is important.

Chapter 2 also provides an overview of the current state of end-user compliance research with the ISP by evaluating existing research to gain insight into the field, depicting the current state of research on end-user compliance with the ISP, identifying gaps, and motivating the need for this research. Furthermore, this chapter will identify existing factors that enhance compliance and components of the conceptual framework based on the literature. Its aim is to address the

first sub-research question (SRQ1): What does existing research reveal about the current state and the factors affecting end-user compliance with the ISP?

2.2 OVERVIEW OF CHAPTER 2

This chapter comprises 4 sections. Section 2.3 outlines the systematic scoping literature review conducted for the study. Section 2.4 discusses the ISP. Section 2.5 discusses end-user compliance with the ISP. Section 2.6 presents a synopsis of approaches used by other researchers to examine end-user compliance with ISPs.

2.3 SCOPING LITERATURE REVIEW

This section provides an overview of scoping literature review as well as how it was applied in this study.

2.3.1 OVERVIEW OF SCOPING LITERATURE REVIEW

A scoping literature review is a method for knowledge production that explores and maps current research on a particular topic. It helps researchers understand what is already known, identify key themes or concepts, and highlight areas where research remains limited or absent (Askey, H. & O'Malley, 2009; Colquhoun et al., 2014). The scoping literature review approach was selected for this study to help the researcher analyse and understand the current state of ISP compliance and identify gaps and develop a framework to improve ISP compliance in government institutions.

2.3.2 IDEAL REPORTING ITEMS FOR SYSTEMATIC REVIEWS AND META-ANALYSIS (PRISMA) METHOD

PRISMA is an evidence-based method with a set of items for reporting on scoping reviews and meta-analysis (Moher et al., 2009). It is used to ensure that the review process is documented. In this study the scoping literature review was guided by the PRISMA framework to ensure a systematic method is followed in the literature review process.

2.3.3 LITERATURE SOURCES

The literature review was conducted using different databases to ensure a wider coverage of relevant literature. The following databases to obtain online articles: Scopus, IEEE Xplore, ACM and Web of Science. The focus was on retrieving academic articles, conference papers, and journals relevant to ISP compliance.

2.3.4 INCLUSION AND EXCLUSION CRITERIA

The inclusion and exclusion criteria were:

Books, book chapters, journal articles, and conference papers were screened for relevance. Publications in English were included. The literature review focused exclusively on articles published from 2009 to 2025 to ensure the most recent and relevant research findings were included, while managing scope and focusing on recent advancements within the field.

The search criteria are summarised in **Table 2-1**. The table lists the keywords used, the databases, the inclusion and exclusion criteria, and the number of relevant publications identified.

Table 2-1: Summary of the Search Criteria

Chapters	Keywords used	Database used	Inclusion principle	Exclusion principle	No of publication
Chapter 2: Literature review	“Information Security Policy Compliance.” “Information Security Policy Compliance Framework.” “End-user compliance with information security policy.” “Factors affecting end-user-compliance to information security policy.” “Factors affecting end-user non-compliance with information security policy.” “Ethics and end-user Compliance to ISP.”	Scopus, Web of Science, ACM, IEEE, Emerald Insight Science Direct Google scholar	Only publications written in English were included. Studies, including models and frameworks for improving information security policy compliance were used. Studies which describe frameworks to improve information security compliance were included. Studies referring to the information security compliance domain were included. Studies referring to information security behaviour were included.	Studies relating to technical protection and compliance tools were not included.	665
Chapter 2 – Literature Review (Grey Literature)	End-user compliance, Information Security Policy, Information Security behaviour reports, Information security in the public sector.	Grey literature sources: Google search, Government websites, Industry reports (e.g., PwC, Deloitte).	Reports, white papers, and publications by reputable organisations relevant to information security policy compliance and behaviour.	Non-credible sources such as blogs, opinion pieces, or non-verifiable online content.	74
Total					739

2.3.5 LITERATURE SEARCH, SCREENING, ANALYSIS AND SELECTION

A total of 665 articles were retrieved from academic databases, including Scopus, IEEE Xplore, ACM, and Web of Science, and exported to Excel for screening. In addition, 74 grey literature sources, such as industry and government reports retrieved via Google search, were included. This brought the total number of retrieved publications to 739.

After removing duplicates, 421 articles were screened for relevance to the research topic; 142 were excluded for failing to meet the criteria. The remaining 279 full-text publications were evaluated in detail, and 197 were excluded using the established exclusion criteria. Consequently, 82 publications met the inclusion criteria and were used in the literature review presented in Chapter 2.

Of these, 50 studies specifically identified and discussed factors affecting end-user compliance with information security policies. These studies were therefore used to extract, group, and categorise the factors that informed the development of the conceptual ECISP Framework.

Figure 2-1 demonstrates the process followed during the search and screening phases.

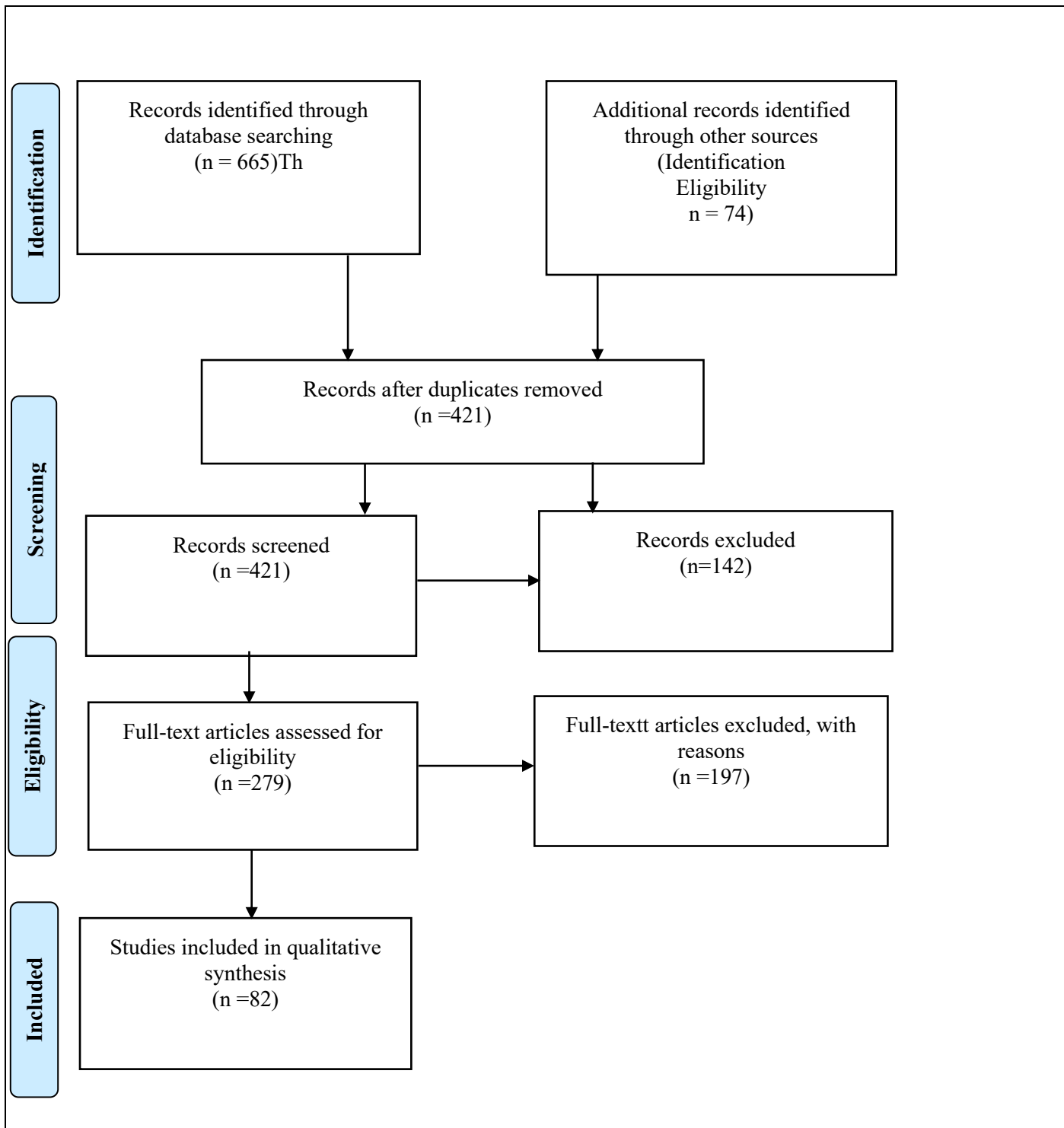


Figure 2-1: Prisma Diagram: Prisma Diagram of Scoping Literature Review

2.4 INFORMATION SECURITY POLICY

This section outlines the purpose and parameters of an ISP, providing a clear definition of this concept within the context of the literature review. Section 2.4 and 2.5 provides background and definition of the concepts of ISP compliance, as well as the importance of ISP compliance, where after the results of the literature review and final papers of the PRISMA are discussed. The results of the PRISMA review is presented in section 2.6

2.4.1 DEFINING INFORMATION SECURITY POLICY

An ISP is defined as:

A formal set of rules, guidelines, and procedures that govern the protection and use of an organization's information assets (Alzahrani, 2021; Balozian & Leidner, 2017; Corpuz, 2011; Kabanda & Mogoane, 2022). ISPs are documents that define the code of conduct, security measures and good practices for information technology and human resources (Hina et al., 2019). ISPs are, moreover, defined as documented, formalised procedures that set out guidelines, roles, and responsibilities by which organisational employees must adhere to safeguard their information technology resources. It specifies the acceptable and unacceptable use of information resources (Kirlappos et al., 2015; Paananen et al., 2020) Yazdanmehr et al. (2024) adds that an ISP is a document that governs human actions related to information security within an organisation.

ISPs are designed to prevent misuse of information and security breaches by employees (Jiang & Zhang, 2023; Lowry & Moody, 2015). It is proposed by Balozian & Leidner (2017) that the ISP should be specific and understandable to employees. Balozian & Leidner (2017) suggest that ISPs' effectiveness is directly linked to employee compliance.

According to Mahmoud (2017) the objective of an ISP is to explain the duties and responsibilities of employees concerning information security. Furthermore, Da Veiga (2015) extends that the ISP is used to guide how employees interact with information assets and subsequently encourages a positive behaviour towards compliance with legislative requirements. It is worth noting that an ISP is an important tool in managing information security. However, while it is essential to develop ISPs, relying solely on the development of

policies is not sufficient to enhance information security in organisations (Bulgurcu et al., 2010; Li & Hoffman, 2023; Parsons et al., 2010).

Information security management is evolving from reliance on only technological and policy development solutions to paying attention to how to improve information security through preventing non-compliance and motivating end-users to comply with IPSs (Alotaibi et al., 2016; Li & Hoffman, 2023; Safa et al., 2016; Son, 2011). The study focuses on the non-technical aspects of information security, namely, behavioural and social factors. The main tool used to address the behavioural and social aspects of information security is the ISP (Alzahrani, 2021; Hedström et al., 2011).

2.5 END-USER COMPLIANCE WITH INFORMATION SECURITY POLICIES

This section outlines a synopsis of the findings from the literature review concerning end-user compliance with an ISP.

2.5.1 DEFINING END-USER COMPLIANCE TO INFORMATION SECURITY POLICIES

End-user compliance with the ISP refers to the extent to which end-users comply with the organisation's prescribed information security rules, procedures, and core security activities. This includes the correct use of security mechanisms such as antivirus software, firewalls, and system updates, as outlined in the ISP (Balozian & Leidner, 2017; Julisch, 2008; Balagopal & Mathew, 2024; Padayachee, 2012).

For the purpose of this study, end-user compliance with an ISP is defined as end-users' adherence to predefined ISP requirements to protect the organisation's information resources. Several organisations experience behavioural information security incidents caused by employees (Yazdanmehr et al., 2024). Most of these incidents are caused by end-users (Ali & Dominic, 2024). As a result, insider threats and non-compliance with an ISP have been regarded as one of the major challenges organisations face (Alraja et al., 2023; Ifinedo, 2012; Li & Hoffman, 2023; Wang et al., 2023). An example of non-compliance with an ISP is an employee who shares his password even though he knows that the policy prohibits him from doing so (Alraja et al., 2023).

2.5.2 THE IMPORTANCE OF END-USER COMPLIANCE TO INFORMATION SECURITY POLICIES

Many organisations invest in information security; however, they continue to experience challenges of data breaches and loss of information (Al-Omari et al., 2013; Bauer & Bernroider, 2017; Khando et al., 2021). Most organisations focus on technological and procedural security measures; however, relying solely on these measures is insufficient to address the challenges posed by information security breaches (Bulgurcu et al., 2010; Faizi & Rahman, 2020). Furthermore, organisations develop ISPs but fail to ensure their implementation by employees (Alotaibi et al., 2016). Organisations need to increase end-user compliance with the ISP to protect Information Security from insider threats (Faizi & Rahman, 2020).

The global state of information security survey 2018 (PricewaterhouseCoopers, 2018) reported that current employees are the most likely source of security incidents in organisations, with an increase of 13% compared to 2016. More recently, the Cybersecurity Insiders (2024) Insider Threat Report found that 83% of institutions experienced insider attacks over the last year. Likewise, the global state of information security survey by PricewaterHouseCoopers (2020) reported that 59% of organisations had experienced a material or significant cybersecurity incident within the preceding 12 months. Organisations continue to face financial and reputational losses due to the potential loss of information stored in their information systems. Beyond data loss, security breaches can cause brand damage and loss of competitive advantage to organisations (CISCO, 2021).

Recent insights from the PricewaterhouseCoopers South Africa Digital Trust Insights Survey (2025) indicated that only 8% of South African organisations reported no severe data breaches over the past three years. This figure is considerably lower than the global average of 18% and the African regional average of 24%, suggesting that South African organisations are more exposed to high-impact breaches than their counterparts elsewhere.

It is therefore worth noting that if employees are non-compliant with the ISP, organisations risk losing critical information and financial assets. For this reason, information security management and ISP compliance have been regarded as some of the key strategic issues in organisations (Alassaf & Alkhalifah, 2021; Al-Omari et al., 2013; Cannoy & Salam, 2010; Stewart & Jürjens, 2017).

It is evident from the above that end-user compliance is one of the key contributors to improving information security in organisations. Developing good policies is futile if users do not comply with those policies. Accordingly, Alotaibi et al. (2016) argue that ensuring compliance with ISP is equally important as having technical solutions at hand. End-user compliance with an ISP is key to the success of information security programs of an organisation (Alassaf & Alkhalifah, 2021; Al-Omari et al., 2012).

2.6 OTHER RESEARCHERS' APPROACHES TO IMPROVE END-USER COMPLIANCE WITH INFORMATION SECURITY POLICIES

In addressing the main research question, “*What elements constitute a framework for end-user ISP compliance within a government institution in South Africa?*”, it is imperative to examine current research on end-user compliance with ISP. SRQ1: *What does the existing research reveal about the current state and factors affecting end-user compliance with the ISP?* Serves as a stepping stone towards addressing the main research question. The subsections below outline the analysis of the current state of end-user compliance with ISP, based on the scoping literature review.

The geographical distribution of the studies, the theoretical frameworks employed by researchers, the validation status of the developed frameworks, the factors identified as influencing end-user compliance with the ISP, and whether the studies targeted government institutions are discussed based on the information extracted from the PRISMA method, refer to **APPENDIX A**. The information is analysed in section 2.6.1-2.6.5.

2.6.1 GEOGRAPHY

Most studies on end-user compliance with an ISP were conducted outside South Africa. **APPENDIX A** shows that only two of the 50 studies that were analysed in this study were conducted in South Africa. The study by Bauer & Bernroider (2017) developed a framework but did not validate it; furthermore, it did not focus on a government institution. The study by Mavetera et al. (2015) focused on a South African government institution; however, no framework was developed.

2.6.2 ENVIRONMENT

Most ISP compliance studies focus on diverse organisations, followed by the banking sector and higher education institutions. Only four of the studies focused on government departments/institutions, namely, studies by (Bauer & Bernroider, 2017; Johnston et al., 2015; Liu et al., 2020; Mavetera et al., 2015). Of those, the studies by Johnston et al. (2015) and Bauer & Bernroider (2017) developed frameworks, but neither was validated.

2.6.3 FRAMEWORK DEVELOPMENT AND VALIDATION

Some studies discuss improving end-user compliance with the ISP without developing a framework. Of the 50 studies analysed, 19 developed a framework. Out of the 19 studies that developed frameworks, 10 validated the frameworks as outlined in **APPENDIX A**. Validation of the framework is important to ensure applicability, usability and suitability within a government institution. Nine of the studies were validated using structural equation modelling (construct reliability, construct validity, convergent validity, and discriminant validity) in SPSS. Only the study by Stewart & Jurjens (2017), which focused on a different organisation in Germany, was validated by field experts through interviews.

2.6.4 THEORIES USED

Table 2-2 depicts the list of theories in order of use, as identified in the studies analysed in **APPENDIX A**.

Table 2-2 : Theories used in Studies

	Theory	No of studies
1.	Theory of Planned Behaviour	17
2.	Deterrence theory	16
3.	Protection motivation theory	13
4.	Social bond theory	6
5.	Theory of reasoned action	4
6.	Rational choice theory	3
7.	Involvement theory	2
8.	Neutralisation theory	2

	Theory	No of studies
9.	Social exchange theory	2
10.	Innovation diffusion theory	2
11.	Organisational justice theory	1
12.	Norm activation theory	1
13.	Universal constructive instructional theory	1
14.	Ethics theory	1
15.	Self-determination theory	1
16.	Organisational control theory	1
17.	Reactance theory	1
18.	Theory on organisational learning	1
19.	Organisational culture theory	1
20.	Situational crime prevention theory	1
21.	Person organisational fit theory	1
22.	Social action theory	1
23.	Social norms theory	1
24.	Social identity theory	1
25.	Dual-process theories of information processing	1
26.	Technology threat avoidance theory	1

Table 2-2 summarises the theories used in the selected sources. The top five theories used in research on end-user compliance in the ISP domain are:

- a) Deterrence Theory – Suggests that undesirable behaviours can be prevented when individuals perceive a high likelihood of severe and swift punishment (Johnson, 2019).
- b) Theory of Planned Behaviour – Describes how a person’s behaviour is mainly determined by their behavioural intent, which is influenced by three basic factors (Zen, 1991):
 - Attitude towards the behaviour: the person’s positive or negative assessment of performing the behaviour.
 - Subjective norms: the observed social influence to perform or not perform the behaviour.
 - Perceived behavioural control: the person’s assessment of the ease or difficulty of performing the behaviour, reflecting both past experiences and anticipated obstacles

- c) Protection Motivation Theory – This theory proposes that people adopt protective behaviours when faced with threats(Addux & Rogers, 1983; Rogers, 1975).
- d) Social Bond Theory – Asserts that people with strong social attachments, commitments, involvement, and belief in societal norms are unlikely to engage in improper behaviour (Ali et al., 2020).
- e) Theory of Reasoned Action – This theory posits that a person’s behaviour is largely driven by their behavioural intent, which is influenced by their attitude towards the behaviour and by subjective norms, the perceived social influence to engage or not engage in the behaviour (Trafimow, 2009).

Theory of planned behaviour was selected as the theory for the conceptual model of this study, as most studies (17 out of 50) in the reviewed literature used theory of planned behaviour.

2.6.5 FACTORS USED/IDENTIFIED

Table 2-3 presents the list of factors that affect end-user compliance with ISP identified from the selected literature sources. Based on the research analysis, the factors were grouped and categorised as outlined in the table. The table shows the category of each factor and the number of times it was identified.

Table 2-3: List of Factors per Category

	Category	Factor	Source	No of Studies
1.	Behavioural motivators-linked to TPB	Self-efficacy	(Ali, Dominic, Emad, et al., 2021 ; Al-Omari et al., 2013 ; Bulgurcu et al., 2010 ; X. Chen et al., 2018 ; X. Chen & Chen, 2016 ; Herath & Rao, 2009 ; Hina et al., 2019 ; Milicevic & Goeken, 2013 ; Nasir et al., 2017, 2019 ; Palanisamy et al., 2020 ; Siponen et al., 2010)	12
2.	Behavioural motivators – linked to TPB	Attitude towards compliance	(Ali, Dominic, Emad, et al., 2021 ; Al-Omari et al., 2013 ; Bauer & Bernroider, 2017 ; Bulgurcu et al., 2010; Foth, , 2017 ; Hina et al., 2019; Ifinedo, 2017 ; Karim et al., 2021 ; Milicevic & Goeken, 2013 ; Nasir et al., 2017, 2019, 2020 ; Sohrabi et al., 2019 ; Sohrabi Safa et al., 2016)	14
3.	SETA	Information security awareness	(Ali, Dominic, Emad, et al., 2021 ; Al-Omari et al., 2012 ; Bulgurcu et al., 2009, 2010 ; Nasir et al., 2017 ; Sohrabi Safa et al., 2016; Sommestad et al., 2014, 2014; Stewart & Jürjens, 2017)	8
4.	SETA	Training and education on IS policies	(Alassaf & Alkhalifah, 2021; Alfawaz et al., 2010; Ali, Dominic, Emad, et al., 2021; Alzahrani, 2021; Bulgurcu et al.,	11

	Category	Factor	Source	No of Studies
			2009; Cannoy & Salam, 2010; Y. Choi, 2017; D'Arcy et al., 2009; Nasir et al., 2017; Siponen, 2010; Stewart & Jürjens, 2017)	
5.	Behavioural motivators-linked to TPB	Normative belief	(Bulgurcu et al., 2010; Herath & Rao, 2009; Karim et al., 2021; Milicevic & Goeken, 2013, 2013, 2013; Nasir et al., 2017, 2019, 2020; Padayachee, 2012; Siponen, 2010; Sommestad et al., 2014)	10
6.	Leadership, management and governance	Organizational commitment	(Ali et al., 2020; Herath & Rao, 2009; Liu et al., 2020; Padayachee, 2012)	4
7.	Behavioural motivators-linked to TPB	Response efficacy	(L. Li et al., 2019 ; Mani et al., 2015 ; Milicevic & Goeken, 2013 ; Padayachee, 2012 ; Palanisamy et al., 2020 ; Rajab & Eydgahi, 2019)	6
8.	Behavioural motivators-linked to TPB	Subjective norms	(Ali, Dominic, Emad, et al., 2021 ; Al-omari et al., 2013; Herath & Rao, 2009; Liu et al., 2020; Milicevic & Goeken, 2013; Rajab & Eydgahi, 2019; Sohrabi et al., 2019)	7
9.	SETA	Previous experience with IS	(Cannoy & Salam, 2010, 2010, 2010; L. Li et al., 2019; Sohrabi Safa et al., 2016)	3
10.	Behavioural motivators	Perceived severity of sanctions	(L. Li et al., 2019; Sohrabi et al., 2019)	2
11.	Behavioural motivators	Belief	(Ali, Dominic, Ali, et al., 2021; Al-Omari et al., 2012; Karim et al., 2021; Siponen & Vance, 2010)	4
12.	Behavioural motivators	Perceived vulnerability	(Ali, Dominic, Ali, et al., 2021; L. Li et al., 2019; Mani et al., 2015; Paananen et al., 2020; Rajab & Eydgahi, 2019)	5
13.	SETA	Involvement of users in IS work	(Ali et al., 2020; Ifinedo, 2017; Karim et al., 2021; Siponen & Vance, 2010; Sohrabi Safa et al., 2016; Sommestad, Karlzén, & Hallberg, 2019)	6
14.	Behavioural motivators	Social pressure/peer behaviour	(Alzahrani, 2021; Cheng et al., 2013; Hina et al., 2019; L. Li et al., 2019; Milicevic & Goeken, 2013a; Siponen & Vance, 2010)	6
15.	SETA	Information security policy awareness	(X. Chen & Chen, 2018; D'Arcy et al., 2009; Mavetera et al., 2015; Siponen & Vance, 2010; Sommestad, Karlzén, & Hallberg, 2019)	5
16.	Behavioural motivators	Attachment	(Ali et al., 2020; M. Choi & Song, 2018; Ifinedo, 2017; Siponen et al., 2010)	4
17.	Behavioural motivators	Response cost	(Ali, Dominic, Ali, et al., 2021; Herath & Rao, 2009; L. Li et al., 2019; Palanisamy et al., 2020; Rajab & Eydgahi, 2019)	5
18.	Behavioural motivators	Threat appraisal	(Dong et al., 2021; Padayachee, 2012; Siponen, 2010; Sommestad et al., 2014)	4
19.	Behavioural motivators	Certainty of sanctions	(Johnston et al., 2017; H. Li et al., 2014; Sohrabi et al., 2019)	2
20.	SETA	Information security knowledge sharing	(Ali, Dominic, Ali, et al., 2021; Karim et al., 2021; Nasir et al., 2017; Sohrabi Safa et al., 2016)	4
21.	Ethics	Personal norms	(Ali, Dominic, Ali, et al., 2021; Ali et al., 2020b; Ifinedo, 2017; Yazdanmehr & Wang, 2016)	4

	Category	Factor	Source	No of Studies
22.	Behavioural motivators-linked to TPB	Perceived behavioural control	(Ali, Dominic, Ali, et al., 2021; Foth, 2017; Hina et al., 2019; Sohrabi Safa et al., 2016)	4
23.	Leadership, management and governance	Organizational culture	(Cannoy & Salam, 2010; Karlsson et al., 2022; Nasir et al., 2019)	3
24.	Leadership, management and governance	Management commitment	(Alassaf & Alkhalifah, 2021b; Ali, Dominic, Ali, et al., 2021; Cannoy & Salam, 2010; Nasir et al., 2019, 2019)	4
25.	Behavioural motivators	Deterrence	(Padayachee, 2012; Siponen et al., 2010)	2
26.	Behavioural motivators	Reducing the rewards for IS misconduct	(Sohrabi et al., 2019a)	1
27.	Behavioural motivators	Certainty of detection	(Foth, 2017a; Herath & Rao, 2009; Milicevic & Goeken, 2013)	3
28.	Behavioural motivators-linked to TPB	Descriptive norm	(Herath & Rao, 2009; Milicevic & Goeken, 2013a; Sommestad et al., 2014a)	3
29.	SETA	Visibility of IS policies/security visibility	(Alzahrani, 2021; Padayachee, 2012; Siponen, 2010)	3
30.	Behavioural motivators-linked to TPB	Coping appraisal	(Ali, Dominic, Ali, et al., 2021; Padayachee, 2012)	2
31.	Leadership, management and governance	Provision of ISP	(Alassaf & Alkhalifah, 2021b; Hina et al., 2019)	2
32.	Behavioural motivators	Employee Commitment	(M. Choi & Song, 2018; Ifinedo, 2017; Sohrabi Safa et al., 2016)	3
33.	SETA	Information security knowledge	(Ali, Dominic, Ali, et al., 2021; Mavetera et al., 2015b; Nasir et al., 2017)	3
34.	Behavioural motivators	Perceived threat susceptibility	(Ali, Dominic, Emad, et al., 2021; Johnston et al., 2015)	2
35.	Behavioural motivator	Perceived ease of use of IS technology	(Al-Omari et al., 2012; Cannoy & Salam, 2010)	2
36.	Behavioural motivators	Increasing the effort for IS misconduct	(Sohrabi et al., 2019)	1
37.	Behavioural motivators	Increasing the risk for IS misconduct	(Sohrabi et al., 2019)	1
38.	Behavioural	Sanctions	(Padayachee, 2012)	1
39.	Other	IS culture	(Ali, Dominic, Emad, et al., 2021; Nasir et al., 2019)	2
40.	Behavioural motivators	Habit	(Ali, Dominic, Ali, et al., 2021)	1
41.	Behavioural motivators	Perceived severity of security breach	(Herath & Rao, 2009)	1
42.	Behavioural motivators	Perceived legitimacy	(Sommestad et al., 2014; Son, 2011)	2
43.	Behavioural motivators	Perceived value congruence	(Sommestad et al., 2014)	2
44.	Behavioural motivators	Cues to action	(H. Chen & Li, 2019; L. Li et al., 2019)	2
45.	Behavioural motivators	Intention to comply	(Foth, 2017a; Wang & Xu, 2021)	2
46.	Behavioural motivators	Perceived effectiveness	(Herath & Rao, 2009; Milicevic & Goeken, 2013, 2013)	2
47.	Behavioural motivators	Perception of controllability	(X. Chen et al., 2018; X. Chen & Chen, 2016)	2
48.	Behavioural motivators	Rewards/incentives	(Cannoy & Salam, 2010; Padayachee, 2012)	2
49.	Behavioural motivators	Motivation	(X. Chen & Chen, 2018)	1
50.	Behavioural motivators	Moral obligation	(Al-omari et al., 2013)	1
51.	Other	Capability	(X. Chen et al., 2018; X. Chen & Chen, 2016)	2
52.	Behavioural motivator	Cost of compliance	(Bulgurcu et al., 2010)	1
53.	Behavioural motivator	Perceived threat severity	(Ali, Dominic, Ali, et al., 2021)	2

	Category	Factor	Source	No of Studies
54.	Leadership, management and governance	Information security collaboration	(Karim et al., 2021; Sohrabi Safa et al., 2016)	2
55.	SETA	Information security intervention	(Sohrabi Safa et al., 2016)	1
56.	Behavioural motivators	Neutralization	(Bauer et al., 2017; Siponen & Vance, 2010)	2
57.	Behavioural motivators	Individual propensity for compliance	(Cannoy & Salam, 2010)	1
58.	Other	Government regulations	(Cannoy & Salam, 2010)	1
59.	SETA	Training on IS technology	(Cannoy & Salam, 2010)	1
60.	Other	Perceived celerity	(Siponen, 2010)	1
61.	Behavioural motivators	Ascription for personal responsibility	(Yazdanmehr & Wang, 2016)	1
62.	Behavioural motivators	Self-regulatory forces	(H. Li et al., 2014)	1
63.	Ethics	Personal ethics	(H. Li et al., 2014)	1
64.	Other	Organizational justice belief	(H. Li et al., 2014)	1
65.	Leadership, management and Governance	Developmental oriented appraisal	(Y. Choi, 2017)	1
66.	Behavioural motivators	Perceived probability of security breach	(H. Chen & Li, 2019)	1
67.	Leadership, management and governance	Cyber security behaviour appraisal	(H. Chen & Li, 2019)	1
68.	Other	Perceived barriers	(H. Chen & Li, 2019)	1
69.	Leadership, management and governance	Poorly managed teams	(Stewart & Jürjens, 2017)	1
70.	Leadership, management and governance	Unskilled management boards	(Stewart & Jürjens, 2017)	1
71.	Leadership, management and governance	Absence of compliance policy	(Stewart & Jürjens, 2017)	1
72.	Behavioural motivator	High level of security breach concern	(Herath & Rao, 2009)	1
73.	Other	Hardware failure	(Stewart & Jürjens, 2017)	1
74.	Leadership, management and governance	Resource availability	(Herath & Rao, 2009)	1
75.	Behavioural motivator	Employees perception of IS security threats	(Ifinedo, 2017)	1
76.	Other	Value conflict between management and users	(Hedström et al., 2011)	1
77.	Behavioural motivators	Perceived justice of punishment	(Sommetstad et al., 2014)	1
78.	Other	Information security policy fairness	(Sommetstad et al., 2014)	1
79.	Leadership, management and governance	Existing organizational formal controls	(Lowry & Moody, 2015)	1
80.	Other	Threats to personal freedom	(Lowry & Moody, 2015)	1
81.	Behavioural motivators	Perceived usefulness	(Al-Omari et al., 2012)	1
82.	Other	Information quality	(Milicevic & Goeken, 2013)	1
83.	Behavioural motivators	Openness to change	(Milicevic & Goeken, 2013)	1
84.	Behavioural motivator	Preventional reasoning	(Milicevic & Goeken, 2013)	1
85.	Behavioural motivators	Social trust	(Milicevic & Goeken, 2013)	1
86.	Behavioural motivators	Sanction rhetoric	(Johnston et al., 2015)	1
87.	Other	Previous incidents	(Mani et al., 2015)	1
88.	Behavioural motivators	Self-disapproval	(Padayachee, 2012)	1
89.	Leadership, management and governance	Information security risk management	(Lowry & Moody, 2015; Nasir et al., 2017; Stewart & Jürjens, 2017)	3
90.	Leadership, management and governance	Appointment of IS managers	(Alfawaz et al., 2010)	1
91.	Other	Formalism	(Al-Omari et al., 2013)	1

	Category	Factor	Source	No of Studies
92.	Behavioural motivators	Benefit of compliance	(Bulgurcu et al., 2010)	1
93.	Behavioural motivators	Cost of non-compliance	(Bulgurcu et al., 2010)	1
94.	Behavioural motivators	Perceived importance of ISP	(Bauer & Bernroider, 2017)	1
95.	Behavioural motivators	Perceived responsibility of ISP	(Bauer & Bernroider, 2017)	1
96.	Behavioural motivators	Perceived IS risk	(Bauer & Bernroider, 2017)	1
97.	Other	New ISP mandatories	(Lowry & Moody, 2015)	1
98.	Behavioural motivators	Anticipated regret	(Sommestad, Karlzén, Hallberg, et al., 2019a)	1
99.	SETA	Organization's IS capability	(Sommestad, Karlzén, Hallberg, et al., 2019a)	1
100.	Behavioural motivators	Perceived demandability fit	(H. Chen & Li, 2019)	1
101.	Behavioural motivators	Perceived need	(H. Chen & Li, 2019)	1
102.	Behavioural motivators	Perceived cost of compliance	(Karim et al., 2021)	1
103.	Other	Size of the organization	(Alzahrani, 2021)	1
104.	Other	Work impairments	(Alzahrani, 2021)	1
105.	Other	Employees anxiety	(Alzahrani, 2021)	1
106.	Other	Continued communication process	(Alzahrani, 2021)	1
107.	Other	Individual's dominant decision style	(Karim et al., 2021)	1
108.	Other	Collaboration between employees	(Karim et al., 2021)	1
109.	Behavioural motivators	Perceived cost of noncompliance	(Karim et al., 2021)	1
110.	Behavioural motivator	Threat severity	(Palanisamy et al., 2020)	1
111.	Behavioural motivator	Perceived deterrent certainty	(Wang & Xu, 2021)(Wang & Xu, 2021)	1
112.	Ethics	Ethical leadership	(Wang & Xu, 2021)	1
113.	Other	Trust	(Alassaf & Alkhalifah, 2021)	1
114.	Other	Security related stress	(Alassaf & Alkhalifah, 2021)	1
115.	Other	Understanding resource vulnerability	(Alassaf & Alkhalifah, 2021)	1
116.	Other	Monitoring (tracking computing activities and performing security audits)	(Nasir et al., 2017)	1
117.	Other	Organizational citizenship behaviours	(Alassaf & Alkhalifah, 2021)	1
118.	Other	Perceived organizational formalization	(Alassaf & Alkhalifah, 2021)	1
119.	Other	Work related groups	(Alassaf & Alkhalifah, 2021)	1
120.	Ethics	Ethical climate	(Alassaf & Alkhalifah, 2021)	1
121.	Other	Organization's information security	(Alassaf & Alkhalifah, 2021)	1
122.	Ethics	Moral beliefs	(Alassaf & Alkhalifah, 2021)	1
123.	Other	Position level	(Alassaf & Alkhalifah, 2021)	1
124.	Other	Satisfaction	(Alassaf & Alkhalifah, 2021)	1
125.	Other	Confirmation of expectations about ISPC	(Alassaf & Alkhalifah, 2021)	1
126.	Other	Security avoidance	(Alassaf & Alkhalifah, 2021)	1
127.	Other	Participation in decision making	(Alassaf & Alkhalifah, 2021)	1
128.	Other	Demographic	(Alassaf & Alkhalifah, 2021)	1
129.	Other	Corporate social responsibility	(Alassaf & Alkhalifah, 2021)	1
130.	Other	Psychological empowerment	(Alassaf & Alkhalifah, 2021)	1
131.	Other	Religiosity	(Alassaf & Alkhalifah, 2021)	1
132.	Other	Internal audit	(Alassaf & Alkhalifah, 2021)	1

	Category	Factor	Source	No of Studies
133.	Intrinsic motivation	Negative experience	(Alassaf & Alkhalifah, 2021)	1
134.	Other	Security agents	(Alassaf & Alkhalifah, 2021)	1
135.	SETA	Informational materials	(Alassaf & Alkhalifah, 2021)	1
136.	Other	Compliance audit	(Alassaf & Alkhalifah, 2021)	1
137.	Other	National culture	(Alassaf & Alkhalifah, 2021)	1
138.	Other	Worries about cyber crime	(Alassaf & Alkhalifah, 2021)	1
139.	Other	Self-regulatory approach	(Alassaf & Alkhalifah, 2021)	1
140.	Organizational culture	Organizational injustice	(Alassaf & Alkhalifah, 2021)	1
141.	Leadership and management	Supervisor subordinate guanxi	(Liu et al., 2020a)	1
142.	Behavioural motivators	Maladaptive rewards	(Ali, Dominic, Emad, et al., 2021)	1
143.	Leadership and management	Psychological capital	(Ali, Dominic, Emad, et al., 2021)	1
144.	Other	Psychological ownership	(Alassaf & Alkhalifah, 2021)	1
145.	Other	Organizational citizenship	(Ali, Dominic, Emad, et al., 2021)	1
146.	Other	Security responsibility	(Ali, Dominic, Emad, et al., 2021)	1
147.	Ethics	Self-morality	(Ali, Dominic, Emad, et al., 2021)	1
148.	Other	Organizational criticality	(Ali, Dominic, Emad, et al., 2021)	1
149.	Other	Perceived impact	(Ali, Dominic, Emad, et al., 2021)	1
150.	Other	Job satisfaction	(Ali, Dominic, Emad, et al., 2021)	1
151.	Ethics	Organizational norms	(Ali, Dominic, Emad, et al., 2021)	1
152.	Leadership and management	Leadership	(Ali, Dominic, Emad, et al., 2021)..(Alassaf & Alkhalifah, 2021)	2
153.	SETA	Levels of ISP knowledge	(Ali, Dominic, Emad, et al., 2021)	1
154.	Other	Organizational behaviour	(Ali, Dominic, Emad, et al., 2021)	1
155.	Other	Psychological contract	(Ali, Dominic, Emad, et al., 2021)	1
156.	Other	Employees status(hierarchal rank)	(Ali, Dominic, Emad, et al., 2021)	1
157.	Ethics	Moral corporate social responsibility	(Ali, Dominic, Emad, et al., 2021)	1
158.	Other	Employment status	(Ali, Dominic, Emad, et al., 2021)	1
159.	Other	Organizational inertia	(Ali, Dominic, Emad, et al., 2021)	1
160.	Other	Individual inertia	(Ali, Dominic, Emad, et al., 2021)	1
161.	Ethics	Values	(Ali, Dominic, Emad, et al., 2021)	1
162.	Leadership, management and governance	Supervisor's support	(Ali, Dominic, Emad, et al., 2021)	1
163.	Other	Extra role behaviours	(Ali, Dominic, Emad, et al., 2021)	1
164.	Other	In role behaviours	(Ali, Dominic, Emad, et al., 2021)	1
165.	Other	Increasing the effort of violation	(Sohrabi et al., 2019)	1
166.	Other	Person organization fit	(H. Chen & Li, 2019)	1
167.	Leadership management and governance	Good organizational governance	(Ali, Dominic, Emad, et al., 2021)	1
168.	Leadership, Management and Governance	Information security monitoring	(Ali, Dominic, Emad, et al., 2021; Amankwa et al., 2022 ; Nasir et al., 2017)	2

The categories that were used to group the factors are:

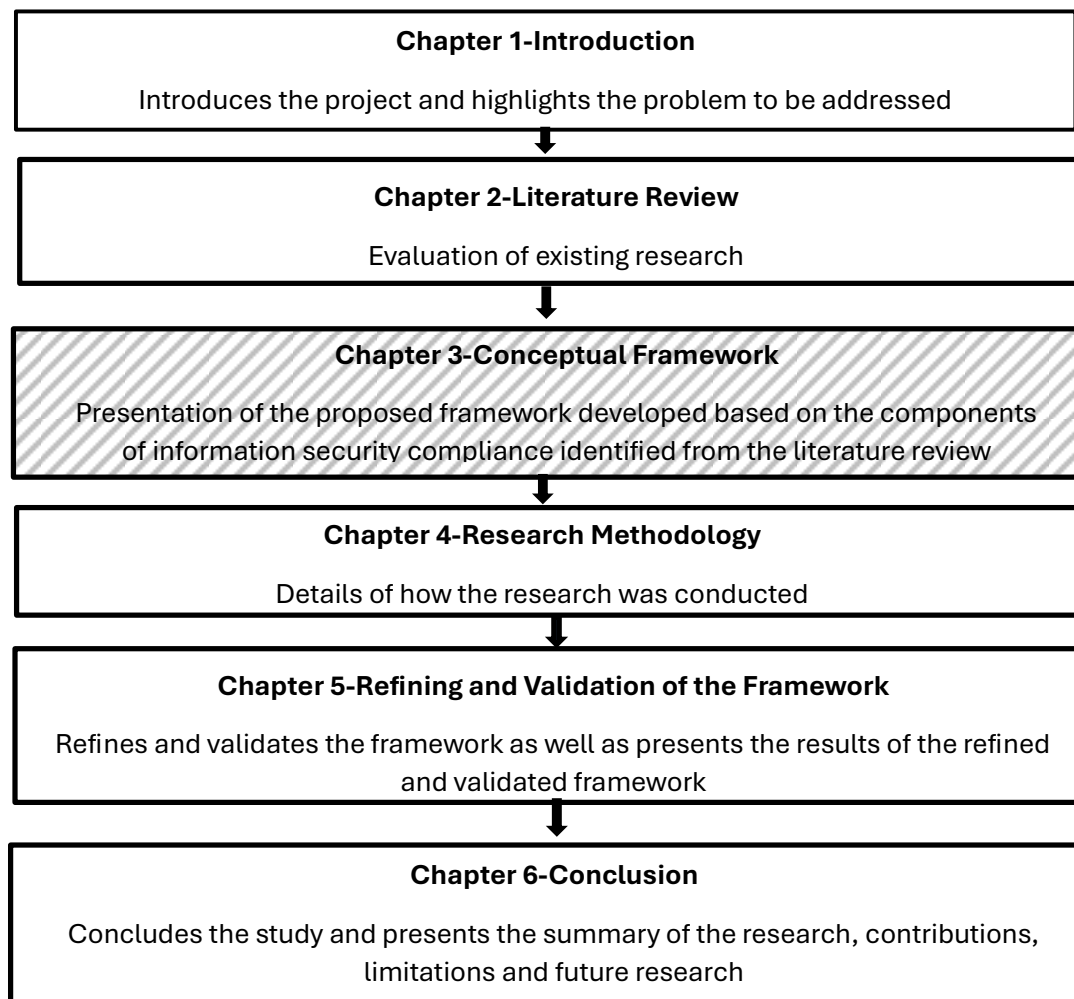
- Behavioural motivators
- Security Education and Training (SETA)
- Leadership, management and governance
- Ethics
- Theory of planned behaviour

The table indicates that 57 factors are related to behavioural motivators, 13 to SETA, 8 to the Theory of Planned Behaviour, 18 to leadership, management, and governance, and 6 to ethics. The information presented in **APPENDIX A** shows that, based on the number of articles focusing on the development and validation of an ISP compliance framework, research in this area is inadequate. Secondly, the number of articles focusing on government departments suggests that research in this area is limited. Thirdly, although some studies focus on government, studies on end-user compliance with ISP that focus on South Africa are lacking. Fourthly, the results show that the most commonly used theories in end-user compliance with ISP are deterrence theory, the theory of planned behaviour and protection motivation theory. Finally, there is no standard framework for improving end-user compliance with the ISP within government departments, given existing policies. This suggests that research on developing a framework for end-user compliance with the ISP within a South African government department is lacking.

2.7 SUMMARY

This chapter aimed to examine the current status of end-user compliance with ISP and related behavioural theories, using a scoping literature review. It also identified the factors that enhance end-user compliance with ISPs by analysing research studies in this domain. This chapter answered sub-research question 1, namely, *What does existing research reveal about the current state and factors affecting end-user compliance with ISP?* The current state was presented in section 2.6.1 – 2.6.4. The current state indicated that out of the 50 studies that were assessed, most of the research were conducted outside South Africa. Furthermore, most of the research covered the private sector, with only two studies conducted in government institutions. Nineteen studies developed a framework, of which 10 frameworks were validated. The theory of planned behavior was the mostly used theory, 17 of the 50 studies applied the theory of planned behavior. The factors were presented in section 2.6.5 and were grouped according to categories, namely; behavioural motivators, SETA, leadership, management and governance, Ethics, and theory of planned behavior. Chapter 3 will present the conceptual framework based on the identified factors and the selected components/categories.

3. CHAPTER 3 THE CONCEPTUAL FRAMEWORK



3.1 INTRODUCTION

In this chapter, the conceptual framework is introduced, representing the proposed solution to the identified problem. This conceptual End-User Compliance with ISP (ECISP) Framework is derived from the literature review described in Chapter 2, which identified factors and theories that enhance end-user compliance with ISPs. These findings from Chapter 2 were used to develop the conceptual ECISP Framework. It provides a preliminary response to the study's main research question: *What elements constitute a framework for end-user ISP compliance within a government institution in South Africa?*

3.2 THE CONCEPTUAL ECISP FRAMEWORK DEVELOPMENT APPROACH

The conceptual ECISP framework was proposed using the components derived from the literature review. The components of a successful framework for end-user compliance with ISP were described, the proposed conceptual ECISP Framework was depicted, and a detailed discussion of its application was provided.

The first component was the selected theory, namely the Theory of Planned Behaviour (TPB). The second, third, fourth, and fifth components were based on the categories chosen to group the identified factors in Chapter 2. The selected categories are:

- Behavioural Motivators
- SETA
- Leadership Management and Governance
- Ethics

3.3 DEFINING A CONCEPTUAL FRAMEWORK

A conceptual framework is a set of interconnected ideas that collectively provide a detailed understanding of a phenomenon or phenomena. The ideas used to establish a conceptual framework support one another, are coherent with the corresponding phenomena, and establish a framework-specific viewpoint. Conceptual frameworks show the relationships among concepts and categories within a subject area and the epistemological assumptions. They are further described as summaries of relationships between components and ideas. They provide common terms and a structure for the variables and recommend assumptions regarding essential associations between the components (Demissew et al., 2015).

3.4 COMPONENTS OF THE FRAMEWORK

Figure 3-1 illustrates the five components and their relationships regarding end-user compliance with the ISP.

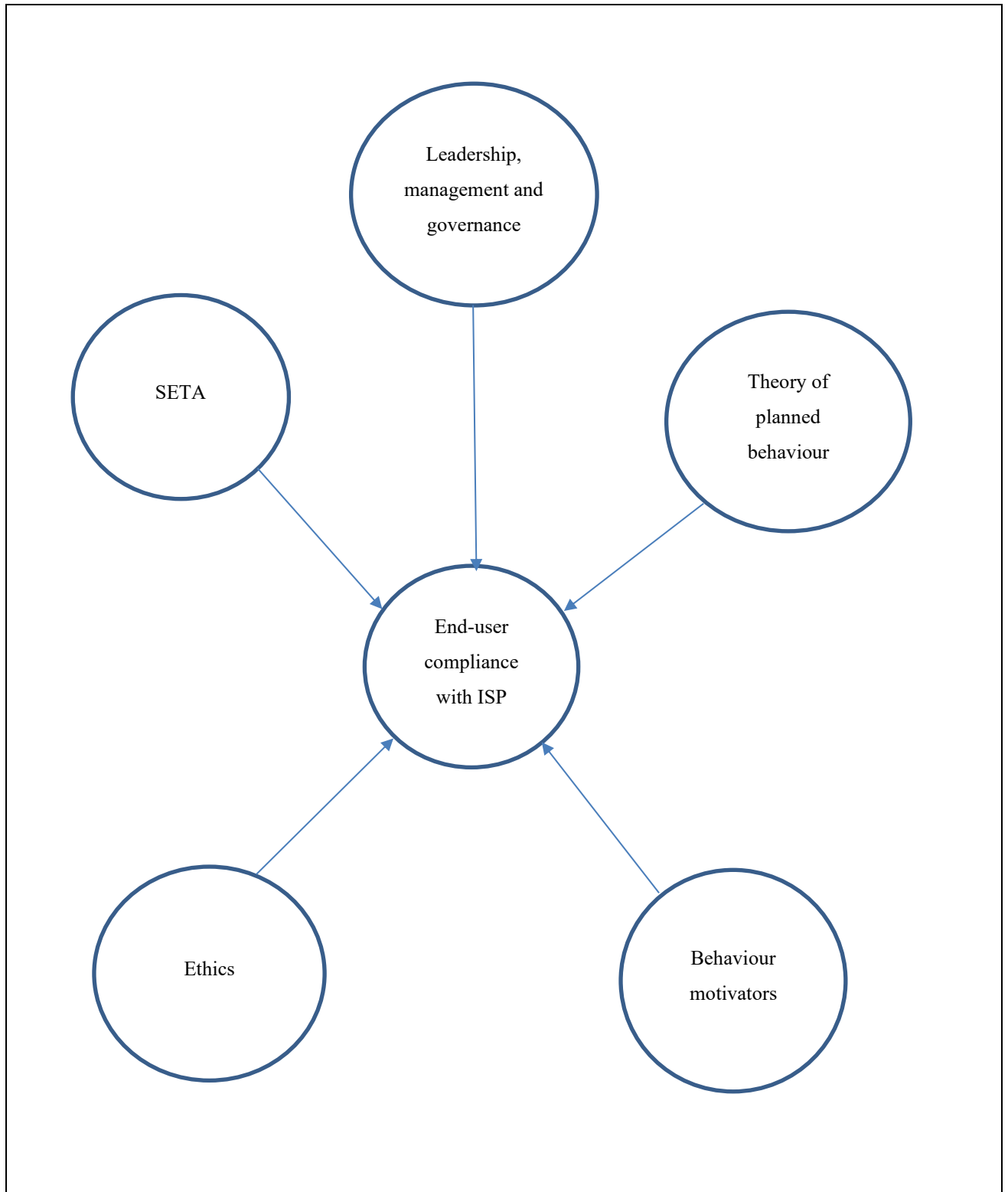


Figure 3-1: The Five Components of the Framework

Based on the findings of Chapter 2, factors and theories relevant to end-user compliance with the ISP were identified through a scoping literature review. A list of 24 theories was identified as outlined in Chapter 2, **APPENDIX A**. Among these, the TPB was selected as a relevant

theory to support the development of the conceptual framework, as it explains how human behaviour is formed and influenced (Ajzen, 1991). This aligns with the purpose of this study, namely, to propose a framework to enhance end-user compliance with ISPs in government institutions. Furthermore, 168 factors were derived from the literature. To build the conceptual ECISP Framework, 32 of the factors were used because they map to the selected categories. Factors were included based on the frequency with which researchers identified them as enhancing end-user compliance with ISPs; only those cited by three or more studies were considered significant enough to be included

Most studies that used the TPB to examine behaviour focused on behavioural intentions. Al-Omari et al. (2013) utilised the TPB to justify users' compliance behaviour with the ISP. Nasiret al. (2017) adopted the TPB to provide a deep understanding and valuable findings regarding ISP compliance behaviour. Sohrabiet al. (2019) used the TPB to develop a conception of how to alleviate the risk of information security transgression in organisations. While Foth (2017) used TPB variables to analyse factors affecting ISP compliance. Karim et al. (2021) on the other hand, combined the TPB, rational choice theory and innovation diffusion theory to propose a research model on employees' decision to comply or not to comply with ISP.

TPB is one of the most well-established theories in the behavioural sciences. It has been recognised as the most significant theory in ISP (Nasir et al., 2020; Sommestad, et al., 2019). Furthermore, it provides a reputable framework for predicting behavioural intentions and actual behaviour (Sommestad et al., 2015). This study examines behavioural factors that enhance ISP compliance, and the TPB has been chosen because it aligns with the study's purpose.

3.4.1 THEORY OF PLANNED BEHAVIOUR

The TPB was selected as one of the framework's components. In Chapter 2, the TPB was identified as one of the most used theories in the information security compliance domain. This theory explains how human behaviour is formed and influenced (Ajzen, 1991). TPB postulates that subjective norms, self-efficacy, and attitude towards compliance influence end-users' intention to comply (Al-Omari et al., 2012; Ifinedo, 2017; Safa et al., 2016).

In Chapter 2, 168 factors that influence end-user compliance with ISP were identified through a scoping literature review. Seven of those factors map to the theory of planned behaviour as outlined in **Table 2-3** in Chapter 2.

Table 3-1 lists the identified factors related to the TPB.

Table 3-1: Factors Related to the Theory of Planned Behaviour

Theory of Planned Behaviour	Subjective norm
	Descriptive norm
	Attitude towards compliance
	Self-efficacy
	Response efficacy
	Coping appraisal
	Perceived behavioural control

3.4.2 ETHICS

Ethics was identified as another component of the conceptual framework because ethical considerations shape end-user behaviour (Roberts, 2021). Employees' moral reasoning and ethical decision-making often determine whether they follow policies (Al-omari et al., 2013). This suggests that, when employees believe that protecting organisational data is the "honourable thing to do", they are more likely to comply voluntarily. Ethics-related factors identified in the literature on moral reasoning, ethical climate, and ethical leadership were found to contribute to an ethical organisation. Furthermore, **Table 3-2** presents a list of six ethics-related factors identified in Chapter 2, which are related to end-user compliance with ISP as outlined in **Table 2-3**. These factors can influence employees' perceptions about organisational policies, procedures, and practices (Saleem et al., 2020).

Furthermore, ethics was selected because it is one of the components that affect compliance with government policies in South Africa. The South African Government, through the Department of Public Service and Administration, has developed policies and frameworks to strengthen measures and standards that promote integrity and ethical conduct in the public service. According to the Department of Public Service and Administration (2013) there is still a challenge regarding compliance with policies and legislation and implementation of ethical

practices in the public sector, with the lack of policy enforcement being regarded as one of the key challenges (Shava & Mazenda, 2021).

Table 3-2: Factors Related to Ethics

Ethics	Ethical leadership
	Personal norms
	Values
	Organisational norms
	Moral beliefs
	Ethical climate

3.4.3 BEHAVIOURAL MOTIVATORS

Behavioural motivators were selected as one component of the framework. The Behavioural Motivators component was established based on an analysis of factors influencing end-user ISP compliance. Factors that directly relate to individual psychological, social, and motivational drivers of behaviour, rather than organisational processes, training, or ethical frameworks, were selected and grouped under the behavioural motivators component. Karimet al. (2021) and Nasir et al. (2019) suggest that behavioural factors significantly affect ISP compliance behaviour. **Table 3-3** presents a list of 57 factors related to behavioural motivators, as identified in Chapter 2, **Table 2-3**.

Table 3-3: Behavioural Related Factors

Information security behaviour	Peer pressure/social pressure
	Attachment
	Threat appraisal
	Certainty of sanctions
	Perceived severity of sanctions
	Belief
	Perceived vulnerability
	Perceived value congruence
	Perceived legitimacy
	Perceived severity of security breach
	Perceived probability of security breach
	Perceived responsibility of ISP
	Perceived deterrent certainty
	Perceived cost of non-compliance
	Perceived cost of compliance
	Perceived need
	Perceived IS risk
	Perceived importance of ISP
	Perceived usefulness
	Perceived justice of punishment
	Perceived ease of use of IS technology
	Perceived threat susceptibility
	Perceived threat severity
	Employee's perception of IS security threats
	Perceived effectiveness
	Openness to change
	Perception of controllability
	Employees commitment
	Habit
	Intention to comply
	Ascription of personal responsibility
	Self-regulatory forces

Individual propensity to comply
Moral obligation
Self-disapproval
Response cost
Deterrence
Reducing the rewards for IS misconduct
Neutralisation
Increasing the effort for misconduct
Increasing the risk of IS misconduct
Sanctions
Cues to action
Rewards/incentives
Motivation
Anticipated regret
Sanction rhetoric
Cost of compliance
Certainty of detection
Preventional reasoning
Benefit of compliance
Cost of non-compliance
High level of security breach concern
Threat severity
Maladaptive rewards
Normative belief
Perceived demandability-fit

3.4.4 SECURITY EDUCATION, TRAINING AND AWARENESS (SETA)

SETA was selected as one of the framework's components. SETA is an essential component of improving an organisation's information security, as it helps change end-user attitudes towards ISP compliance (Cox, 2012). Implementing SETA programmes is crucial in motivating employees to comply with the ISP. (Hina et al., 2019). Furthermore, information security awareness affects employee attitudes (Karim et al., 2021), and attitudes are directly related to the Theory of Planned Behaviour, as they are among the variables of TBP (Sommestad et al.,

2019). Factors under SETA were identified in the literature, highlighting training, education, and awareness as key drivers of ISP compliance. These factors were grouped together because they focus on equipping employees with the necessary knowledge, skills, and awareness to recognise risks and comply with ISP. **Table 3-4** presents a list of 15 factors related to SETA as identified in Chapter 2, **Table 2-3**.

Table 3-4: SETA Related Factors

Security Training, Education and Awareness	Training and education on ISP
	Information security awareness
	ISP awareness
	Previous experience with information security
	Information security knowledge sharing
	Involvement of users in IS work
	Visibility of IS policies
	Information Security Intervention
	Informational materials
	IS knowledge
	Organisational IS capability
	Levels of ISP knowledge
	Training on IS technologies

3.4.5 LEADERSHIP, MANAGEMENT AND GOVERNANCE

Leadership, management and governance were selected as another component of the framework because of their important role in ensuring ISP compliance. A study conducted by Koohanget al., (2020) suggests that leadership, management and governance are important elements that affect employees' intent to comply with ISP requirements in organisations. Good security management, appropriate security awareness, a strong security culture and positive management behaviours improve end-user ISP compliance. Furthermore, management is responsible for improving information security compliance in organisations (Ali et al., 2021). Factors in this category were identified from studies highlighting organisational influence, leadership and management behaviour, and governance in achieving ISP compliance. **Table 3-5** presents a list of 20 factors related to leadership, management, and governance, as identified in Chapter 2, **Table 2-3**.

Table 3-5: Leadership, Management and Governance

Leadership, Management and Governance	Organisational commitment
	Organisational culture
	Management commitment
	IS risk management
	IS climate
	IS collaboration
	Effective leadership
	Good organisational governance
	IS monitoring
	Resource availability
	Absence of compliance policy
	Cyber security behaviour appraisal
	Development-oriented appraisal
	Existing organisational formal controls
	Provision for ISP
	Unskilled management boards
	Supervisor-subordinate guanxi
	Management behaviour
	Leadership

3.5 THE CONCEPTUAL ECISP FRAMEWORK

This section describes the proposed conceptual ECISP Framework. It provides a summary of how the conceptual framework is generated and of the components integrated to form the initial conceptual framework.

3.5.1 THE APPROACH TO CONCEPTUAL FRAMEWORK DEVELOPMENT

The scoping literature review in Chapter 2 aimed to unpack components that could inform the conceptual framework. The focus was on identifying the factors that enhance end-user compliance to ISP, identifying theories within the information security domain that have an impact on end-user compliance to ISP, and identifying applicable South African components that affect ISP compliance APPENDIX A.

An initial conceptual framework for end-user compliance with an ISP within a government department with an existing ISP was developed based on the components derived from consolidating the selected factors, relevant theories, and ethics, which were identified as a distinct component.

The conceptual framework included only factors cited by three or more researchers from the list shown in **Table 2-3**, and from the categories of the Theory of Planned Behaviour, Security Education, Training and Awareness, Behavioural Motivators, and Leadership, Management and Governance. This ensures that it comprises relevant, commonly identified factors, thereby increasing its reliability and relevance. The categories were used to group related factors and to determine linkages between them (**Table 3-1** to **Table 3-5**). Subsequently, the categories were used to formulate the components of the proposed framework. Each component comprises the factor within its category. For the ethics category, all identified factors were included, even those cited by fewer than three researchers, because few studies directly linked ethics to ISP compliance.

Ethics was maintained as a distinct component because ethical challenges remain a concern within the South African government context. The different factors were then mapped to show their relationship with end-user compliance with an ISP. Based on the analysis and mapping of the factors with the components, a total of 33 factors were used to develop the conceptual framework.

3.5.2 ILLUSTRATING THE CONCEPTUAL ECISP FRAMEWORK

As indicated in section 3.2, a conceptual framework is a summary of relationships among components and ideas. The initial framework, as presented in Error! Reference source not found., illustrates the process and the identified components. This conceptual framework is regarded as the *Framework for End–User Compliance to ISP within a Government Institution*.

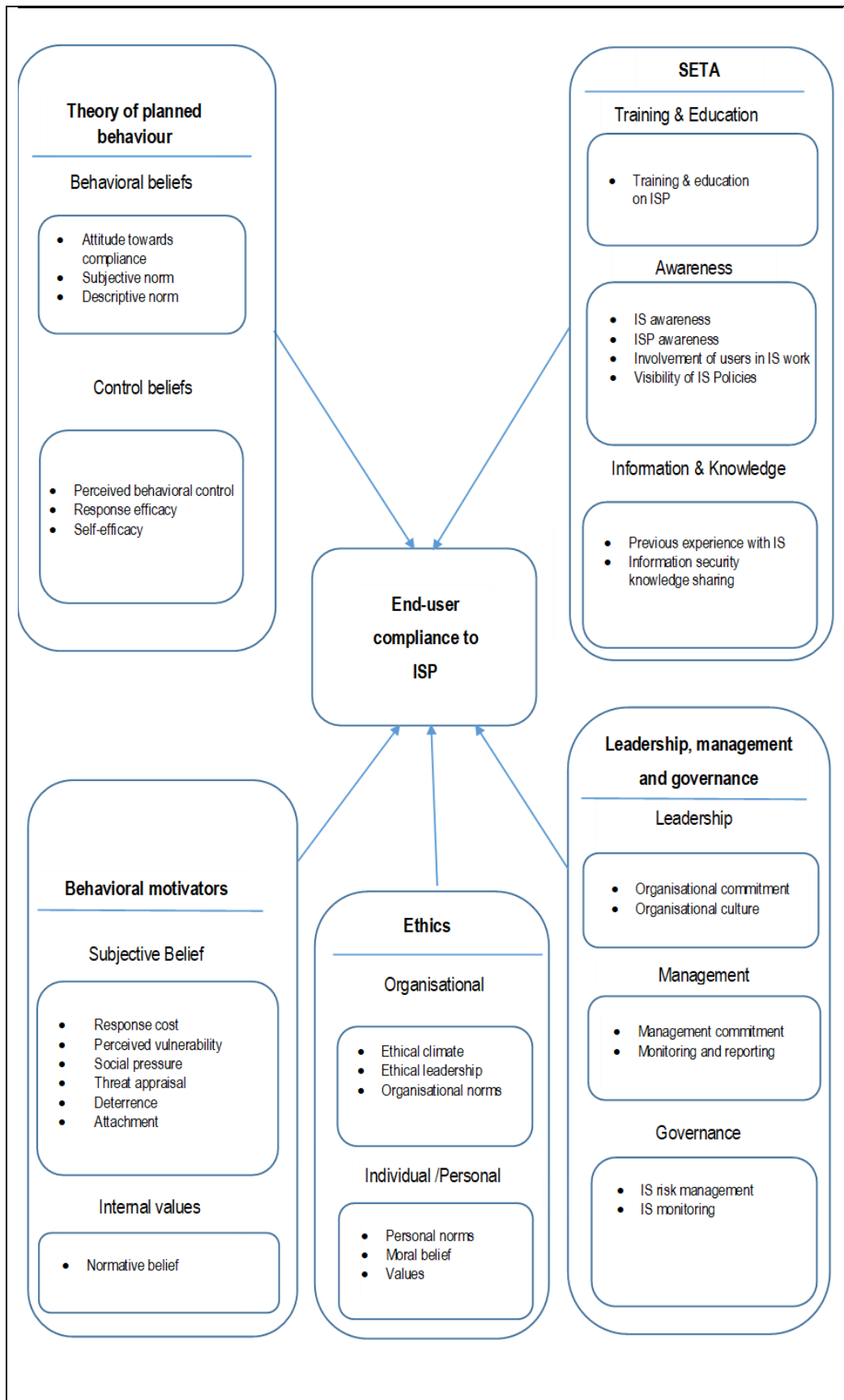


Figure 3-2: The Conceptual Framework

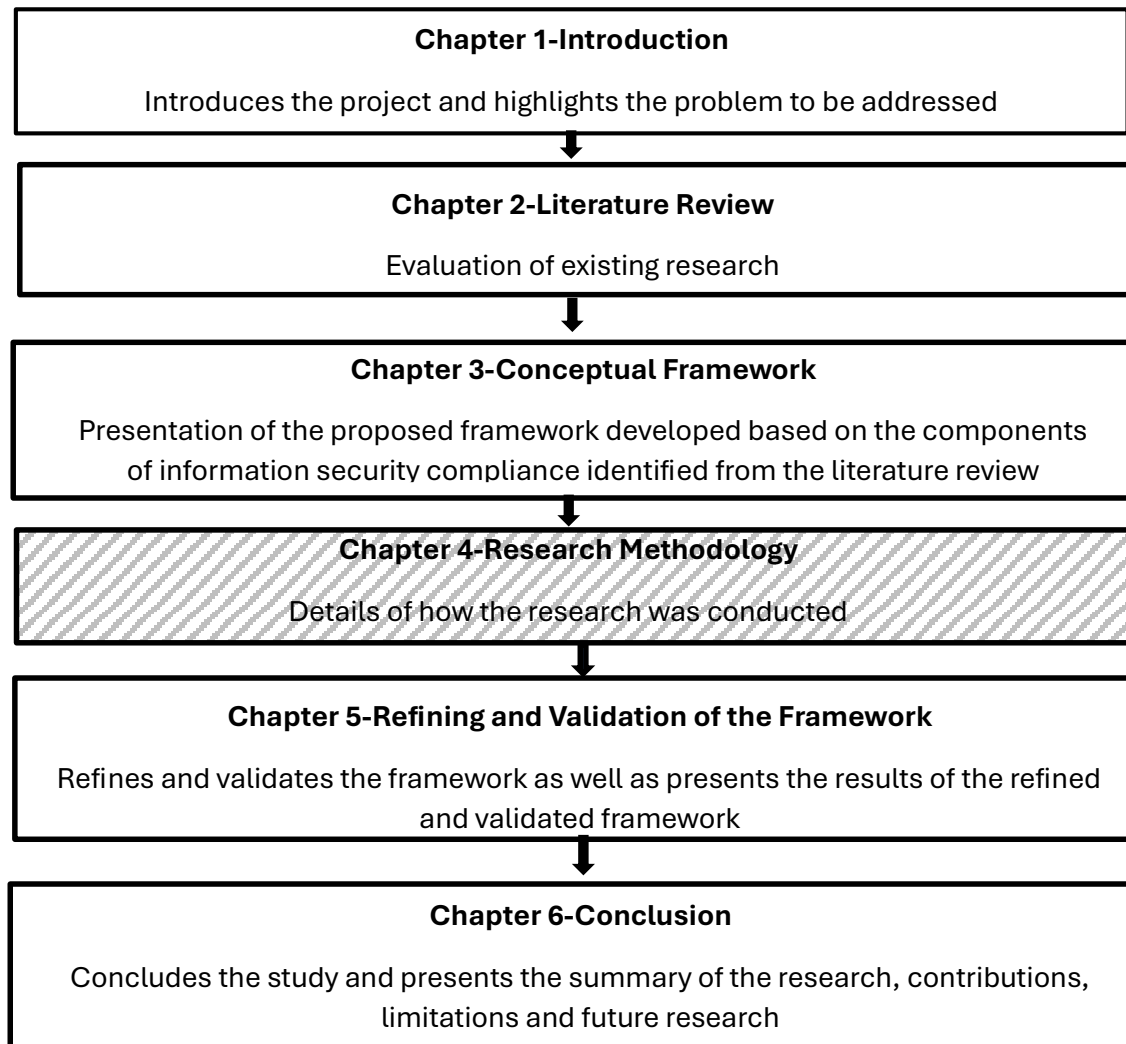
The conceptual framework illustrates the relationship between the identified components and the factors that enhance end-user compliance with ISP in government institutions. Each component, derived from the categories established during the literature review, serves as a building block that collectively contributes to the development of the conceptual ECISP Framework. The framework provides a structured view of how behavioural, organisational, ethical, and educational aspects interact to enhance end-user compliance with ISP compliance. It forms the foundation for the subsequent refinement and validation processes discussed in the following chapter.

3.6 SUMMARY

The primary objective of this study is to develop a framework that enhances end-user compliance with ISPs within a government department, as shown in **Error! Reference source not found..** This chapter introduced the components of the framework, derived from the literature reviewed in Chapter 2. These components include the Theory of Planned Behaviour, Ethics, Security Education, Training and Awareness, Behavioural Motivators, and Leadership, Management and Governance, together with the factors associated with each. The framework was then constructed to illustrate the relationships among these components and factors, and how they collectively contribute to enhancing end-user compliance with IPSs.

Chapter 4 outlines the research methodology, which describes the methods and techniques used to collect and analyse data. It explains the research design, sampling techniques, data collection methods, data analysis techniques and the ethical considerations applied in the research study. It includes the interview process and expert reviews, and explains how these will help further refine and validate the proposed ECISP Framework.

4. CHAPTER 4: RESEARCH METHODOLOGY



4.1 INTRODUCTION

This chapter outlines the research methodology used in this study to address the research questions. A systematic approach is used to move from a research problem to a resolution (Creswell, 2014). Therefore, the aim of this chapter is to outline the research approach used in this study. The chapter provides a perspective on the research design process, outlining the research philosophy, research approach, and research strategies used in this study. It also outlines the three phases of the case study, as adapted from (Yin, 2003). Furthermore, the chapter explains the data collection, analysis and validation techniques applied in the study.

4.2 RESEARCH DESIGN PROCESS

The research onion, as described by Saunders et al. (2009), is considered a suitable framework for defining a research methodology. For that reason, the research onion was used as a guide to explain the selected method for this research study. **Figure 4-1** illustrates the research onion.

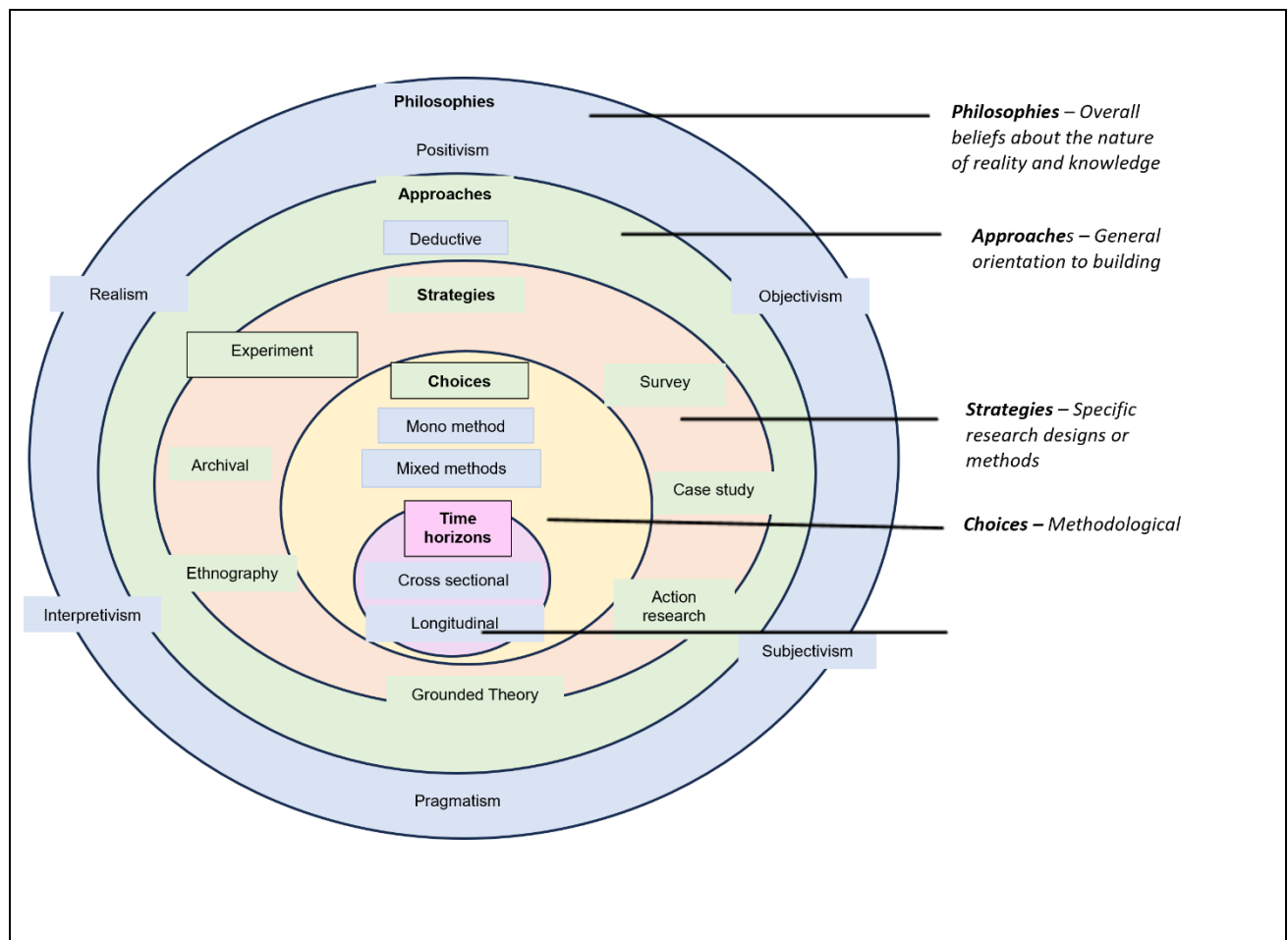


Figure 4-1: Research Onion

Source: Adapted from (Saunders et al., 2018)

The research onion comprises six layers, each representing a specific research choice. Using the research onion, the researcher proceeds from one layer to another, starting with the outer layer. The research onion offers numerous options within each layer. This section will discuss the research choices selected for this study. Each layer shown in **Figure 4-1** is explained in the subsequent subsections.

4.2.1 RESEARCH PHILOSOPHY

A research philosophy is described as the assumptions about how people view the world (Saunders et al., 2015). A researcher's assumptions about the world view contribute to the choice of research strategy and method. Furthermore, understanding research philosophy contributes to knowledge development about how the data used to develop the knowledge should be gathered (Saunders et al., 2015).

Saunders et al. (2015) pinpoints three fundamental philosophical assumptions, which are;

- Epistemology – relates to what makes up adequate knowledge in the field of study.
- Ontology – relates to researchers' assumptions about how the world functions and to their commitment to certain opinions.
- Axiology – focused on the role of a researcher's values in the research process.

There are four primary philosophies, namely: realism, positivism, interpretivism, and pragmatism.

- **Realism:** Realism assumes that a reality exists that is autonomous of human thoughts, perception, and emotions (Saunders et al., 2015).
- **Positivism:** Positivism is the philosophical perspective that is accepted by natural scientists (Saunders et al., 2019). This philosophical stance is selected if the researcher chooses to work with visible and measurable social reality (Gcaza, 2017).
- **Pragmatism:** Pragmatism recognises the research question as the most important factor in deciding which research philosophy to adopt (Saunders et al., 2009, 2015).
- **Interpretivism:** Interpretivism emphasises the value of understanding the social actors related to a phenomenon as a significant part of conducting research (Creswell, 2007). Interpretivism postulates that researchers interpret the roles of social actors in line with the interpretations of those roles (Saunders et al., 2015).

Interpretivism was considered a suitable philosophy for this study. This approach enables the researcher to gain an understanding of the phenomenon through questioning, observation and interpretations (Gcaza, 2017). This philosophy is deemed suitable for the following reasons:

- The study aims to develop an ECISP Framework that assists organisations in improving employee compliance with their ISP, namely, human behaviour.

- The development of the framework is informed by an understanding of the participant's point of view (Ryan, 2018). In this case, the interviews with government officials (IS professionals) and the expert interviews.
- The study interprets the meanings that social actors (information security professionals and experts) ascribe to the phenomena.
- Adopting the interpretivism approach allows the study to acquire a deeper understanding of the interpretations of the information security professionals of the ECISP Framework.
- The probable assumptions for this study are adapted from Creswell (2009), presented in **Table 4-1** to illustrate the choices made when adapting the interpretivism philosophy.

Table 4-1: Interpretivist Assumptions: Adapted from (Cresswell 2009)

Assumptions	Question	Characteristics	Implications for this study
Ontological	What is the nature of reality?	Reality is subjective, and participants in the study may have different ideas of it.	The researcher asks open-ended questions to elicit diverse views from participants, based on their experiences and perspectives. This assists the researcher in acquiring a deeper comprehension of the participant's subjective reality.
Epistemological	What is the relationship between the researcher and the researched subject?	The researcher is a subjective participant observer who cannot be separated from the research.	The researcher shares their interpretation of the data with participants and seeks feedback to ensure it accurately reflects participants' perspectives.
Methodology	What is the research process?	The researcher uses inductive reasoning to generate reliable data that is used to build a theory.	The researcher uses a qualitative method, conducting interviews to systematically collect and analyse data, determine patterns and themes, organise the data into meaningful categories, and refine the proposed framework.

In interpretive research, the foundation is based on interpretation in order to understand the phenomena from the social actor's point of view (Saunders et al., 2015). The goal of this study is to develop an ECISP Framework to enhance end-user compliance with ISP in government institutions.

4.2.2 RESEARCH APPROACH

Research studies involve the use of theories, and the link between theory and reality is perceived through the research approach (Bryman, 2004). There are three essential research approaches recommended in the research onion, specifically, induction, deduction and abduction (Saunders et al., 2015). A deductive research approach is initiated by a theory, whereby data is collected to examine the theory (Gcaza, 2017). This approach is quantitative in nature. An inductive approach is based on the observation and analysis of data, whereby data is used to develop a theory, as seen in **Table 4-2** (Gcaza, 2017; Saunders et al., 2015). An abductive approach is based on collecting data to explore a phenomenon, identify themes, and patterns to generate a new or modify an existing theory that is subsequently tested through additional data collection (Saunders, 2023).

Table 4-2: Characteristics of Inductive, Deductive and Abductive Approaches, adapted from Saunders et al. 2015; and Saunders 2023

Deductive	Inductive	Abductive
Theory is followed by data.	Data is followed by theory.	Data and theory are used together to generate a new or modify an existing theory.
Rigid - uses a highly structured methodology.	A flexible, less-structured approach permits alternative explanations of the phenomena.	Permits exploration of data, and testing through subsequent data collection.
Concerned with what is happening.	Concerned with the context.	Concerned with the specific and the general.
Quantitative.	Qualitative in nature.	Qualitative.
Findings are generalised.	Findings are less generalisable.	Known premise is used to generate testable conclusions.
Tests hypothesis.	Less concerned with the requirement to generalise.	Concerned with generating testable conclusions.
The researcher is detached from what is observed.	The researcher is linked to the process.	The researcher moves iteratively between data and theory.
Concepts need to be operationalised.	Investigates research context.	Existing concepts and new findings are combined and refined.
Follows a reductionism principle.	Uses a bottom-up approach.	Use a back-and-forth approach.
Appropriate for large samples.	Appropriate for a study of a small sample.	Suitable for studies that focus on data interpretation and theory refinement throughout the process.

An abductive approach is more suitable for qualitative research. It is suitable for this study because it is flexible and allows the researcher to better understand the nature of the problem (Saunders et al., 2015). Furthermore, the study uses a small sample to enable the researcher to explore the participants' experiences and perspectives in depth, and it aligns with the characteristics of an inductive research approach as outlined in **Table 4-2** above. A qualitative research approach involves interpreting data to understand the meanings individuals ascribe to it and the methods used to generate it for analysis. It is an explanatory, realistic approach to the world (Creswell, 2007; Creswell & Poth, 2016; Kennedy, 2019; Quinn Patton & Cochran, 2007).

Creswell et al. (2016) and Creswell (2007) identify several characteristics of qualitative research, as outlined in **Table 4-3**.

Table 4-3: Characteristics of Qualitative Research

Characteristic	Description	Application in this study
Natural setting.	Data is collected in the field where participants experience the issue under study.	Data is collected from IS professionals within a government institution and from IS experts, ensuring authenticity and reflecting participants' experiences.
Researcher as a key instrument.	Researchers collect data through an instrument they developed and through direct interaction with participants.	The researcher uses interview questions developed by him/her and personal interaction with participants to gather data. The interview questions are based on theory and literature to ensure they are relevant and valid for the study.
Multiple data collection methods.	The researcher collects various forms of data.	The researcher collects data using interviews with government officials and expert reviews to assess and validate the proposed framework. The collected data were analysed and organised into categories and themes using the thematic analysis method.
Inductive and deductive data analysis.	Researchers use a bottom-up approach to analyse data and build themes that are constantly checked against the data.	The researcher uses an inductive approach to data analysis and develops a set of themes from the collected data. These themes are continually checked against the collected data to ensure they are mutually exclusive and meaningful, thereby refining the components of the conceptual ECISP Framework.
Participants' multiple perspectives and meanings.	The focus is on the participants' perspectives.	Data is collected on the views of IS professionals and experts.
Context dependent.	The research is situated within the context of the participants.	The researcher seeks to understand the circumstances within the government institution that influence ISP compliance behaviour.
Emergent design.	The research plan is tightly prescribed.	The research process is open to change, allowing the researcher to learn from participants and respond accordingly.
Reflexibility.	Researchers convey their background and how it informs their interpretation of the study's information.	The researcher conveys their work experience and how it informs their interpretation of the information gained from the study.
Holistic account	Researchers develop a complex picture of the problem.	In-depth analysis of the factors influencing ISP compliance.
Theoretical lens	Using existing theory related to the study.	The relevant literature was reviewed to provide a solid foundation for the study. The researcher uses the theory of planned behaviour to identify factors that influence end-user compliance. These factors are used to develop the proposed ISP Compliance Framework.
Interpretive inquiry	The researcher interprets what is observed, heard and understood.	The researcher translates the results through thematic analysis, identifying themes and patterns.

This study is qualitative, and the next section discusses the research strategy.

4.2.3 RESEARCH STRATEGIES

Saunders et al. (2009) define a research strategy as a plan that describes how the researcher embarks on answering the research questions. The research strategy enables the researcher to determine a suitable method to address the research problem (Saunders et al., 2009).

Saunders et al. (2009) considers seven research strategies, namely:

- Experiment – is usually applied in natural sciences and used to study links between variables.
- Survey – is associated with a deductive approach and is mostly used to answer quantitative questions.
- Case study – involves practical analysis of a specific concept using various sources of evidence. It is of interest to researchers seeking answers to the 'why', 'what', and 'how' questions. It is typically used in explanatory and exploratory studies.
- Action research – focuses on actions related to promoting change in an organisation. It involves both data gathering and change facilitation.
- Grounded theory – uses data generated from a sequence of observations to develop a theory.
- Ethnography – is firmly rooted in the inductive approach. It is used to explain participants' perspectives on their social world.
- Archival research – uses administrative data and documents as the primary source of information.

When identifying the most suitable study strategy, it is suggested that a researcher should first consider the research purpose (Gcaza, 2017). Saunders et al. (2009) proposes that a researcher should be guided by the following elements when choosing a suitable research strategy:

- The research question(s) and objectives.
- The amount of time and other available resources.
- The researcher's own philosophical foundations.
- The level of existing knowledge in the subject area under investigation.

Table 4-4 outlines the characteristics of the different research strategies in order to identify the appropriate strategy for this study. The research questions serve as column headings, and the research strategies and their characteristics are listed in rows. Each characteristic's relevance to the research questions is demonstrated by a tick.

Table 4-4: Characteristics of Research Strategies, adapted from Cresswell (2007)

Strategy	Characteristics	Source	What elements constitute a framework for end-user ISP compliance within a government institution?	What does existing research reveal about the current state and factors affecting end-user compliance with ISP?	How can the existing literature help constitute a framework for end-user compliance for ISP?	What elements constitute a validated framework for end-user ISP compliance within a government institution?
Experiments	Experimental group and control group.	(Saunders et al., 2009)				
	Conducted in a laboratory setting.					
	Studies causal links between variables.					
Survey	Associated with a deductive approach.					
	Exploratory and descriptive research.					
	Large amounts of data.					
	Questionnaire					
	Structured observation.					
Case study	Empirical investigation.	(Creswell et al., 2016; Saunders et al., 2009)		√	√	√
	Multiple sources of evidence.		√	√	√	√
	Interviews, observation, questionnaires.					√
	Explanatory and exploratory.		√	√	√	√
	Holistic treatment of the phenomenon.		√	√	√	√
Action research	Concerned with the resolution of organisational issues. Involvement of practitioners. Iterative process. Implications beyond the immediate project. Multiple data generation methods. Action outcomes and research outcomes. Concentration on practical issues.	(Oates, 2006; Saunders et al., 2009)				
Grounded theory	Meaning emerges from a phenomenon.	(Saunders et al., 2009)				
	Data Collection and analysis are simultaneous.					
	Theory is derived from data.					
Ethnography	The researcher spends time in the field.	(Oates, 2006; Saunders et al., 2009)				
	Natural setting.					
	The researcher is the research instrument.					
	The researcher constructs an illustration of the world as participants observe it.					√
	The researcher produces a holistic description of the cultural aspects of the situation.					
Archival research	Uses administrative records and documents.					
	Secondary data analysis.					
	The researcher determines what data are available and designs the research to make the most of them.					

Based on the above, a case study is deemed the most suitable approach for this research. A case study focuses on a single item to be investigated, and examines it thoroughly using a range of data collection methods (Oates, 2006). A case study allows the researcher to gain a deeper understanding of the phenomenon being investigated, and to respond to the ‘why’ and ‘how’ questions (Oates, 2006; Saunders et al., 2009).

There are two kinds of case studies, namely, single and multiple case studies (Gustafsson & Gustafsson, 2017; Yin, 2003). A single case study is used to test whether a theory’s recommendations are correct or whether further explanation might be necessary (Saunders et al., 2009). Furthermore, a single case study enables the researcher to gain a deeper understanding of the phenomena being explored and to question old theoretical relationships to discover new ones. (Gustafsson & Gustafsson, 2017; Saunders et al., 2009a; Yin, 2003).

This study uses a single case study to examine the suitability of the proposed conceptual framework for end-user compliance with an ISP within a government institution. The study was conducted in three phases; each phase informs the next. The three phases were adopted from the Yin case study method (Yin, 2003). Yin describes the case study research method as an iterative process in which each phase is linked to the others. Furthermore, each phase requires the researcher to review former decisions. The phases are outlined in **Figure 4-2**, including how the chapters fit within each phase of the study. For each chapter, the focus, research approach and final deliverable are depicted.

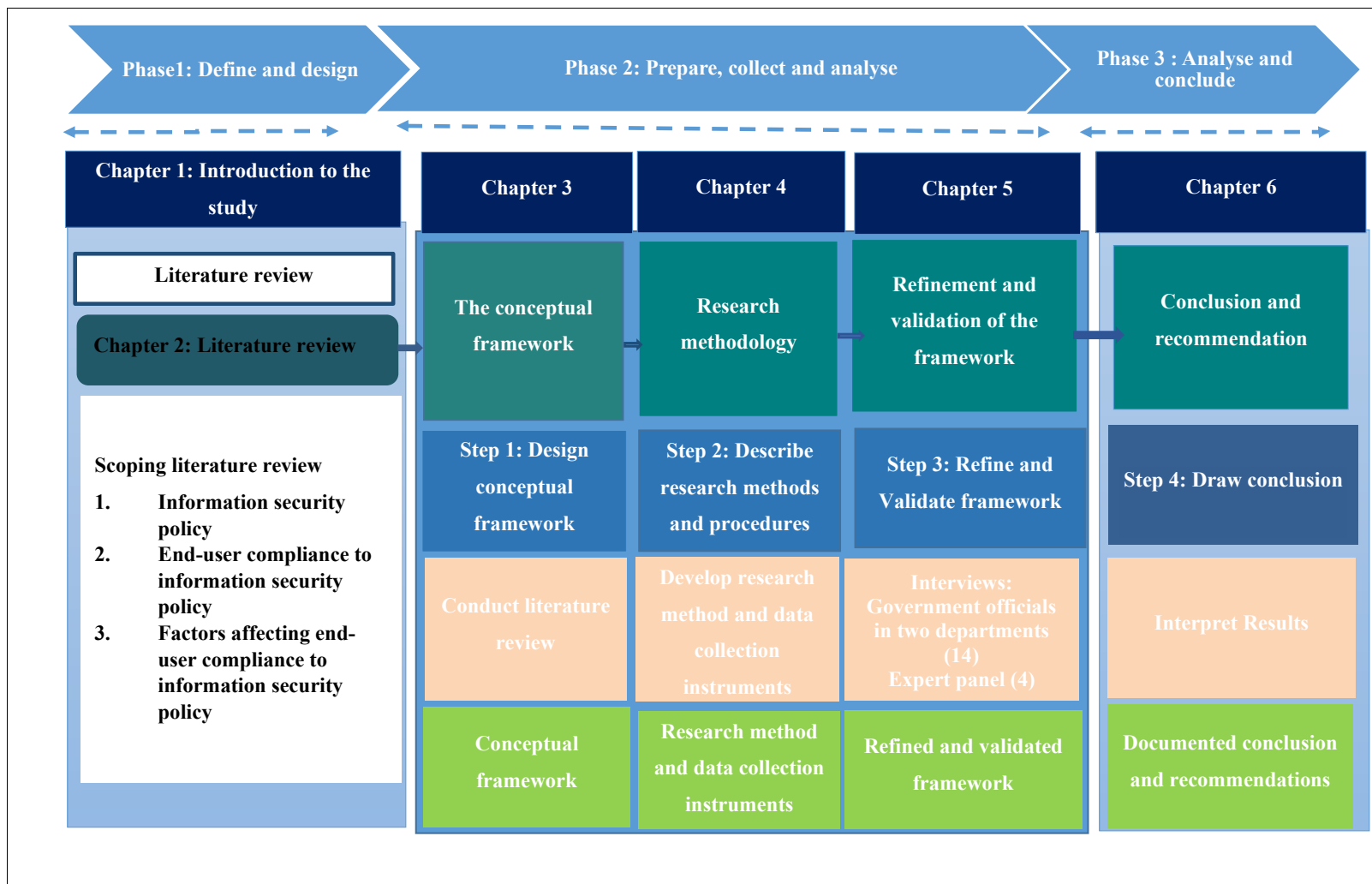


Figure 4-2: Phases of the Study, adapted from Yin (2003)

4.2.3.1 *Phase 1: Define and design*

Yin (2003) describes this phase as identifying the examined theory in the case study. In this study, the literature review phase outlines the factors that affect end-user compliance with an ISP. This phase is presented in Chapter 2, which assesses the relevant literature to identify the components of the proposed framework. Chapter 2 answers SRQ1: *What does existing research reveal about the current state and factors affecting end-user compliance with the ISP?*

4.2.3.2 *Phase 2: Prepare, collect, and analyse*

This phase describes the preparation for data collection, the principles of data collection, and the data analysis strategy. The outcomes of this phase are presented in Chapters 3, 5, and 6. Chapter 3 develops the conceptual ECISP Framework using the identified components. Chapter 3 aims to answer SRQ2: *How can the existing literature help constitute a framework for end-user compliance with the ISP?*

Chapter 5 aims to answer SRQ 3: *What elements constitute a validated framework for end-user ISP compliance within a government institution?* Chapter 6 aims to answer the main RQ: *What elements constitute a framework for end-user ISP compliance within a government institution?*

4.2.3.3 *Phase 2 – Step 1: Conceptual Framework*

Step one of the research study involves developing the conceptual ECISP Framework through a thorough literature review and determining its components from the reviewed literature (Chapters 2 and 3). The literature review enables the researcher to gain an in-depth understanding of the existing knowledge and theories relevant to the research problem. It also helps the researcher identify gaps in existing knowledge that the research study can address. Based on the findings from the literature review, the researcher identified the components of the conceptual ECISP Framework. This phase informs the development, refinement and validation of the conceptual ECISP outlined in the subsequent stages of the research process.

4.2.3.4 *Phase 2 – Step 2: Describe the research method and procedures*

Step 2 of the research study outlines the research approach (Chapter 4), presenting the methods used to collect and analyse data, along with the software employed. Chapter 4 presents the sample and the sampling technique employed to select participants. The chapter further outlines the steps taken to ensure the study's validity and reliability.

4.2.3.5 *Phase 2 – Step 3: Refine and validate the framework*

Step 3 of the research study focuses on refining and validating the conceptual ECISP Framework. In this phase, the framework is refined by government officials and validated by information security experts through online interviews. Government officials were selected to refine the framework because they understand their environment and they will be able to advise on whether it would be suitable for applying in government departments. The purpose of the refinement is to confirm whether the conceptual ECISP Framework is suitable, usable, complete, and applicable to improving end-user compliance within a government institution. Experts were selected because they possess knowledge and experience to assess whether the framework is relevant for its intended use. The validation aims to evaluate the proposed framework and determine its accuracy, comprehensiveness, relevance, and effectiveness.

4.2.3.6 *Phase 2 – Step 3- 1: Refine framework: Interviews with government officials*

Interviews with government officials were conducted to refine and assess the proposed framework. A purposive sample of officials was identified through the researcher's professional network. Semi-structured interviews were conducted using open-ended questions informed by the research objectives and framework components. The aim was to gather qualitative insights into the framework's suitability and usefulness in a government context. Interviews were conducted online, recorded, and later transcribed for analysis using Atlas.ti. Feedback from participants informed the refinement and enhancement of the framework components.

4.2.3.7 *Phase 2 – Step 3 -2: Validate framework: Expert Interviews*

Interviews were conducted with experts in ISP compliance to validate the proposed ECISP Framework and assess its accuracy, comprehensiveness, relevance, and effectiveness within a government institution. A sample of experts in information security and compliance was identified through professional networks and online platforms to ensure participation by highly qualified individuals with relevant experience. The experts were selected for their knowledge of ISP compliance. The interviews were conducted online using a semi-structured approach. The questions were open-ended to elicit comprehensive feedback and gather recommendations for improvement.

The interviews were conducted online and audio-recorded. The interview data were transcribed and analysed using Atlas.ti. The interview input was the refined framework and its components. The interview feedback was used to refine the ECISP and to develop a validated ECISP Framework.

4.2.3.8 *Phase 3 – Step 4: Conclusion and Recommendation*

This phase presents the final ECISP Framework to improve end-user compliance in a South African government institution. It also provides conclusions and recommendations regarding areas of concern that could hinder the effective application of the ECISP Framework to improve end-user compliance with the ISP in South African government institutions.

4.2.4 DATA COLLECTION TECHNIQUES

Various instruments are used to collect data when conducting a research study.

Table 4-5 presents the frequently used data collection instruments used by researchers.

Table 4-5: Frequently Used Data Collection Instruments

Data collection instruments	Source	Advantage	Disadvantage	Applied in this study
Questionnaires	(Oates, 2006)	Cost-effective. Easy for participants to fill in and easy to analyse. Few geographical limits. No need to have special social skills for the self-administration questionnaire.	Pre-defined answers can cause frustration. The researcher cannot query disparities between answers. The researcher cannot correct misunderstandings.	No
Interviews	(Creswell, 2007; Oates, 2006)	Good at tackling topics in detail. Little equipment is required. The researcher can check whether the participant is the correct person to answer the questions. Flexible Participants often enjoy the opportunity to talk about their ideas.	Time consuming Possibility of a lack of reliability. Possibility of being misleading. They are unnatural. Need suitable social skills. Not appropriate for circumstances where a researcher wants to make generalisations about an entire population.	Yes
Observation	(Oates, 2006)	Uncovers what people actually do, as opposed to what they report to be doing. Collects large amounts of quantitative data quite quickly. Generates data on objects that many participants are unaware of. Cost-effective. Provides means to get intense insights into social situations. Enables researchers to discover people's views and intentions as they see them.	Restricted to studying overt behaviour. Not easy to give feedback to people who were observed. Anything that happens in the absence of the observer is unknown. A researcher can lead researchers into risky areas. Sometimes criticised for lack of reliability. Not easy to generalise from observations in one situation to others.	No

4.2.4.1 Interviews - Government Officials

Interviews are conversations between people that help the researcher obtain legitimate and trustworthy data relevant to the research question and objectives (Gustafsson & Gustafsson, 2017; Saunders et al., 2009). Interviews are suitable for studies that aim to gather detailed information, ask complex questions, and investigate sensitive issues. They are mostly used in case studies and ethnographies (Oates, 2006).

During the interviews, the five components of the conceptual ECISP Framework were demonstrated, along with their respective factors. The conceptual ECISP framework was included in the interview guide. The demonstration involves presenting a prototype or model in a controlled environment to show how it functions in addressing real-world problems (Hevner et al., 2004). This process enables stakeholders to interact with the framework, evaluate its usability, and provide actionable feedback based on their professional experiences. The conceptual ECISP framework was presented to the participants during the interview sessions, before the interview questions were asked.

Demonstration is important in case study research as it helps the researcher gain a better understanding of how theoretical constructs perform in practice. It also allows the researcher to validate the framework by applying it in specific contexts. Yin (2003) points out that such a process improves the robustness of the findings by linking empirical evidence to theoretical propositions. Demonstration also ensures that the artefact (in this case, the conceptual ECISP Framework) is usable and effective in practice (Peffer et al., 2007).

In this study, interviews were used to refine and validate the proposed ECISP Framework. Feedback from participants was used to determine whether the components of the proposed ECISP Framework are suitable, complete, and applicable. A semi-structured interview approach was used to interview government officials. A set of open-ended interview questions was developed based on the study's research questions and objectives. By engaging government officials in this process, the framework's institutional relevance was confirmed, and its completeness and usability were tested against real-world challenges.

4.2.4.2 Expert reviews - Interviews

Expert reviews are important for validating a model and enhancing the credibility and the reliability of the research (Richey et al., 2014; Kakar et al., 2023). Expert reviews are used in

phase 2 of the case study method. Four domain experts were requested to assess and evaluate the proposed ECISP Framework.

According to Ericsson & Smith (1991) and Caley et al. (2014), an expert is a person who has relevant skills and special knowledge in a particular area and has the ability to critically evaluate information. A sample of four experts in information security was selected based on their knowledge and experience. The selected experts have at least five years of relevant experience in information security. They have knowledge of information security policies and frameworks. Furthermore, they have experience working within a government institution. The experts assisted in validating the proposed ECISP Framework to determine whether it is comprehensive, accurate, and relevant. The feedback from the expert reviews was used to refine the ECISP Framework and develop a final, validated end-user ISP compliance framework.

4.2.5 SAMPLE SELECTION

According to Creswell (2014), the selection of a sample size in qualitative research should be guided by the principles of achieving data saturation and obtaining information-rich cases. Similarly, Creswell (2014) and Creswell, et al. (2016) recommends a sample size of 20-30 participants for most qualitative studies. Furthermore, Guest et al. (2006) suggests that saturation can be achieved with as few as 3-6 participants in qualitative research studies, such as expert validation. In this study, a sample of 14 government officials from two departments in the Mpumalanga Province was selected. Participants were identified from the Information Technology and Security Management divisions.

Table 4-6 presents a list of the government officials who participated in the evaluation and of the framework.

Table 4-6: Government Officials' Roles and Years of Experience

Government Official	Area of Work	Years of Experience
Official 1	Security	15 - 20 years
Official 2	Information Technology	15 - 20 years
Official 3	IT Governance	15 - 20 years
Official 4	Security	5 - 10 years
Official 5	Information Technology	15 - 20 years
Official 6	Information Systems	10 - 15 years
Official 7	Information Technology	10 - 15 years
Official 8	Security	15 - 20 years
Official 9	Information Technology	5 - 10 years
Official 10	Information Systems	15 - 20 years
Official 11	Information Technology	5 -10 years
Official 12	Information Technology	5 - 10 years
Official 13	Information Technology	5 - 10 years
Official 14	IT Governance	5 - 10 years

Furthermore, four information security experts were selected to participate in the expert review phase. The experts were selected from the field of information security, with a focus on those with experience working within government institutions. The selection criteria included a track record of implementing security frameworks in the public sector.

The following criteria were used to select the experts:

- A minimum of five years of experience in information security, with consideration of inviting experts with most experience in information security in the targeted government institution.
- Experience implementing information security governance frameworks and policies within the public sector.
- Knowledge of end-user behaviour and compliance challenges in government settings.

To identify information security experts, the researcher used a combination of professional networks and online platforms. One expert is an information security specialist who is a member of the National GITO Council. This expert worked for one of the National departments and contributed to the development of several National Information Security Policies in South Africa. This expert was approached directly due to a prior professional relationship with the researcher. Furthermore, this expert was asked to recommend other colleagues in the field. LinkedIn was also used to identify additional information security experts. The researcher assessed profiles based on experience, certifications, and contributions to the field.

Table 4-7 outlines the information security experts who participated in validating the ECISP Framework.

Table 4-7: Experts' Knowledge Domain and Years of Experience

Expert Reviewer	Knowledge Domain	Years of Experience
Expert Reviewer 1	Development of National Information Security Policies	5 - 10 years
Expert Reviewer 2	Information Security Framework Design and Implementation	10 - 15 years
Expert Reviewer 3	End-User Compliance and Security Awareness Programmes	15 - 20 years
Expert Reviewer 4	Risk Management and Government IT Systems Security	10 - 15 years

In this study, the following reasons support the use of 14 participants from two government departments and four experts:

Data Saturation – The primary goal of qualitative research is to reach data saturation, at which point collecting additional data yields no new insights. Initially, 25 government officials were identified across three departments. However, only 14 agreed to participate in the study, and formal approval to conduct the research was granted by only two departments. The third department did not respond despite multiple follow-ups. By recruiting 14 participants from government departments, the research aims to gather diverse perspectives from the IT and Security management divisions. The qualitative, open-ended interviews enabled the researcher to gather more information on end-user compliance with the ISP in government institutions.

Using 3-5 experts to validate the refined ECISP Framework can provide sufficient data to achieve saturation. Guest et al. (2006) asserts that a smaller sample size may be appropriate when participants have extensive knowledge of the subject matter. Additionally, conducting interviews with 3-5 experts enables the researcher to conduct in-depth interviews and analyse the feedback thoroughly within time constraints.

Information-Rich Cases – Creswell (2007) point out the importance of selecting participants who can provide rich, detailed information relevant to the research question. The selected participants are likely to provide meaningful data on end-user compliance with the ISP and to help confirm the suitability, applicability, and usability of the proposed ECISP Framework.

Purposive Sampling – Creswell (2007) suggests that purposive sampling is the most appropriate approach for qualitative research. The researcher selected participants from the IT and Security management divisions in each department. This enabled the researcher to gather valuable data from individuals with experience in the subject matter.

Practical Considerations – Creswell (2007) notes that time, resources, and feasibility are key in determining sample size. The selection of 14 participants from two government departments in Mpumalanga province was based on the availability of participants within the IT and Security management divisions. Furthermore, the sample size was affected by the IT division's status in Mpumalanga province. Most departments have fewer IT employees, which limits the pool of potential participants. Given these constraints, using 14 participants is reasonable and balances data saturation with practical feasibility.

4.2.6 DATA COLLECTION

In this study, data were collected through semi-structured online interviews with government officials and information security experts, conducted via Microsoft Teams. The interview questions were designed in line with the research objectives, research questions, and the components of the proposed ECISP Framework. The questions were shared with participants in advance to allow adequate preparation. Participants' consent was obtained to audio-record the sessions to ensure data accuracy and completeness.

4.2.7 DATA ANALYSIS

Data analysis was conducted to identify relationships in the data and draw conclusions (Creswell, 2007; Oates, 2006). In this study, non-statistical data were collected. Data analysis involves scrutinising, categorising, organising, and testing the evidence to address the primary study intentions (Creswell, 2007; Oates, 2006; Saunders et al., 2019; Yin, 2003). Braun & Clarke (2006) mention various types of data analysis such as content analysis, thematic analysis and grounded theory. This study uses thematic analysis to analyse the data.

Creswell's (2007) six-step process, which provides a systematic approach to analysing interview data, was used as follows:

1. Organising and preparing data: The interview audio recordings and transcripts were transcribed. The transcribed data were organised and labelled for easy access throughout the analysis.
2. Reading and reviewing data: The researcher read and reviewed the data to interpret the content and assess its meaning.
3. Coding data: The researcher organised the collected data according to codes. The codes were allocated to specific words and phrases related to the research question.
4. Developing categories and themes: The researcher reviewed the coded data and identified the categories and themes.
5. Validating findings: The researcher sought feedback from participants to confirm the accuracy of the findings derived from the data.
6. Writing up the results: Lastly, the researcher captured the interpretation of the findings and the implications of the results.

4.2.7.1 Data Analysis Tools Used in This Study

The researcher used Atlas.ti 25 to analyse the data. This software is an effective tool for qualitative data analysis. Atlas.ti can handle textual, graphical and multimedia formats (Archer et al., 2017).

The data collected through open-ended interviews were interpreted and coded using qualitative data analysis (Braun & Clarke, 2006). Braun and Clarke (2006) six-phase thematic analysis approach was applied as follows:

Phase 1: Data familiarization: The researcher read and re-read the transcripts to understand the data.

Phase 2: Generating initial codes: The researcher reviewed the transcripts to identify patterns, codes, and categories within the data.

Phase 3: Searching for themes: The researcher grouped similar codes together to develop themes.

Phase 4: Reviewing themes: After establishing the themes, the researcher reviewed and refined the themes to ensure they align with the assigned codes and organised them into different categories.

Phase 5: Defining and naming themes: The researcher defined and named the themes in line with the codes.

Phase 6: Producing the report: The researcher interpreted the themes and presented them in chapter 05, supported by quotations from participants.

4.2.8 DATA VALIDITY AND RELIABILITY

An abductive theory was used in the data analysis to ensure data reliability. This approach involves a systematic method for analysing data. Abductive theory is used to explore and test data through subsequent collection; it uses known premises to generate testable conclusions. It can be used in qualitative research, which applies the systematic identification of patterns, themes, and categories in the data to generate new, modify an existing theory (Savarit, 2020; Saunder, 2023).

The interviews were transcribed, and the researcher read them to understand the data. Key phrases or themes were identified, coded and analysed. *Member-checking* is a technique described by Lincoln & Guba (1985). This method is used to improve data credibility by

communicating research findings to participants to seek clarification or validation, ensuring that their views are accurately captured.

Dependability was ensured through the accurate recording and transcription of interviews. Transferability was enhanced by providing a detailed description of the research context and methods. Verbatim quotes were provided to support the findings and ensure authenticity.

4.2.9 INTERVIEW BIAS

- Interview bias is when the expectations and behavior of the interviewer influences the responses of participants Zahle (2024). To avoid interview bias, the following mitigations were considered;
- A structured, standardized interview guide was used and shared with participants prior to the interview.
- All participants were interviewed separately to ensure individual responses.
- All participants were asked the same questions in the same order to avoid interview discretion.
- The importance of participants' inputs in improving the ECISP framework was emphasized.
- Interviews were recorded to ensure accurate capture of participants responses.

4.3 INTERVIEW GUIDE

Interview guide was developed based on the conceptual ECISP Framework and its components. The purpose of the interview guide is to provide guidance for the interview and to ensure that interviewers assist the researcher in gathering relevant data that addresses the research questions. The interview questions were informed by the components and factors of the conceptual ECISP framework that were identified from literature review.

4.3.1 INTERVIEW GUIDE FOR GOVERNMENT OFFICIALS – REFINEMENT

The interview with government officials focused on the following aspects:

1. **Suitability:** Confirms whether the conceptual ECISP Framework aligns with the requirements of government institutions to ensure end-user compliance with ISP.

Confirming the suitability of a framework through interviews is crucial to ensure it fits the purpose. Maucoet al. (2020) confirmed an e-health readiness framework for developing countries, verifying that it aligns with local contexts, stakeholder expectations, and real-world constraints. Confirming the suitability of the ECISP Framework helps ensure it aligns with the requirements of South African government departments.

2. **Usability:** Determines whether the framework is user-friendly and can be easily implemented within the government institution. Lee & Lee (2022) points out that confirming usability is important to ensure that a framework is suitable for its intended use.
3. **Completeness:** Confirms whether all essential components and elements are included in the conceptual ECISP Framework. Bohnsacket al. (2014) asserts that, to increase the potential for success, a business model should be complete and account for all relevant factors.
4. **Applicability:** Evaluates whether the framework is easy to apply in government institutions. The study by Abliz et al. (2020) assessed the factors influencing end-user compliance with information security policies in organisations, thereby supporting the verification of the framework's applicability.

4.3.2 INTERVIEW GUIDE FOR EXPERT REVIEW – VALIDATION

The expert interviews focused on the following areas:

1. **Accuracy:** Assess the correctness of the components of the conceptual ECISP Framework. Confirming the framework's accuracy through expert review improves its reliability. A study by Alenezi et al. (2019) used expert interviews to verify and refine a proposed framework, adding missing factors and ensuring it reflected real-world issues.
2. **Comprehensiveness:** Assesses whether the ECISP Framework includes all essential components required to enhance end-user compliance with the ISP framework. The comprehension of policies and frameworks increases the success of ISP implementation (Bulgurcu et al., 2010).
3. **Relevance:** Verifies whether the proposed ECISP Framework and its factors address challenges relevant to government institutions. Alenezi et al. (2019) demonstrate that assessing a framework's relevance can help determine whether it can be adopted and implemented in a specific context.

4. **Effectiveness:** Assesses whether the proposed ECISP Framework is successful in achieving the desired results. Alenezi et al. (2019) conducted interviews with experts to ensure it was complete, accurate and effective.

The interview guide was developed to obtain responses from the participants, which were used to refine and validate the proposed ECISP Framework. See **APPENDIX E** and **APPENDIX F**.

4.4. LIMITATIONS

The framework refinement was conducted through interviews with staff at two government institutions in Mpumalanga Province, and validation was conducted through interviews with four experts. The findings may be limited to the Mpumalanga Government and the experience of the experts used. The results may not represent a holistic view of the matter under review.

4.5 ETHICAL CONSIDERATIONS

In any research study, it is crucial to consider the ethical implications of the research design, methodology, and data collection. Participation in this study is voluntary. Ethical considerations were made in accordance with the University of South Africa (UNISA) ethics policy. The researcher obtained ethical clearance from UNISA's ethics committee, under certificate reference number 2036.

Ethics approval documents (**APPENDIX B:** and the permission letters from the government institutions (**APPENDIX C**) are attached. Participants signed consent forms for participating in the study.

Ethical considerations were carefully addressed to ensure participants' rights were protected. Ethical issues were addressed during and after the research.

The research took note of the following:

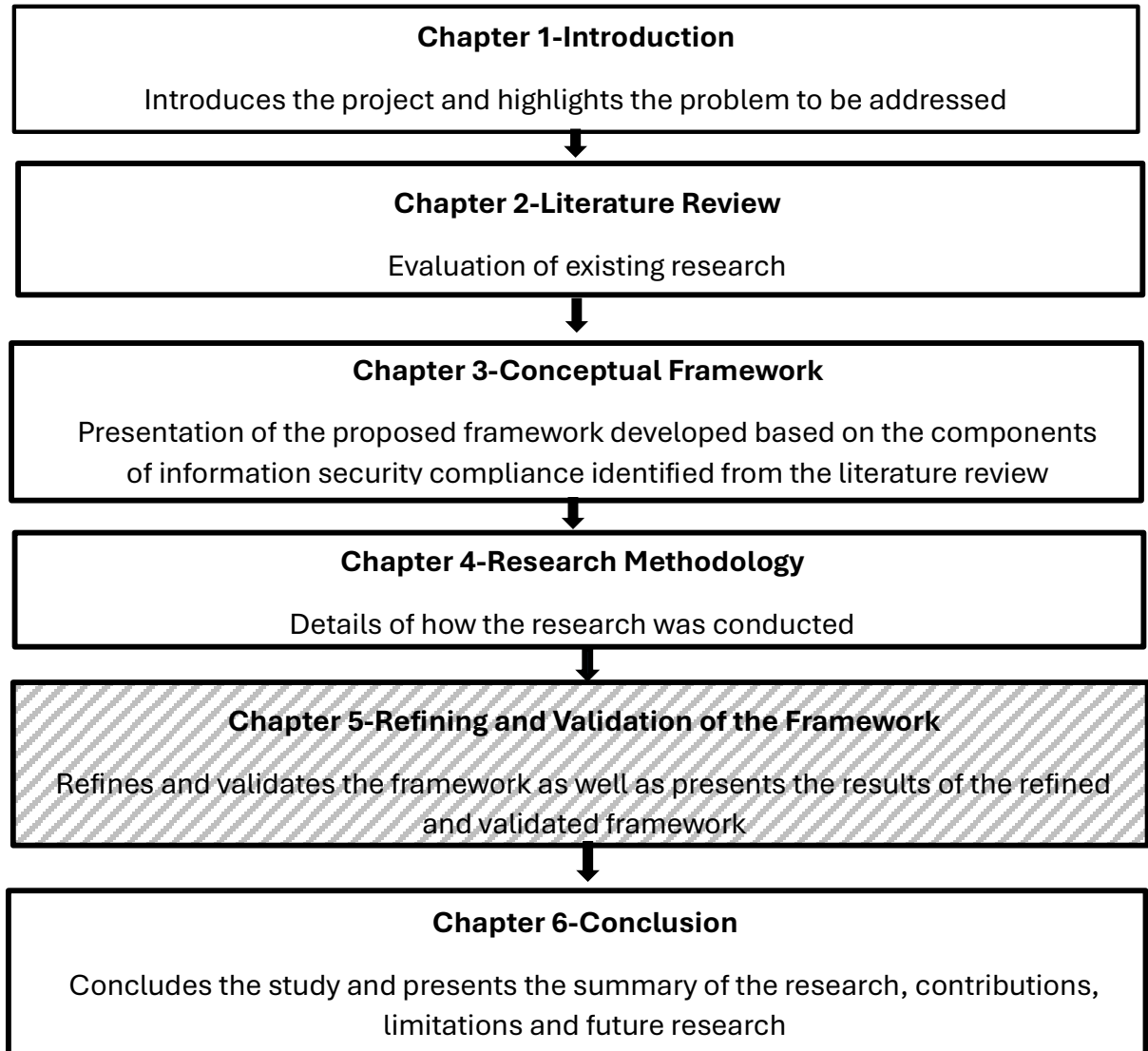
- The participants were notified about the purpose of the study and participated voluntarily.
- Confidentiality and anonymity of the participant were ensured.
- These rights of participants were provided and read out to the participants, and they confirmed that they understood their rights before any of the evaluation began.

- Participants were voluntarily included in the research after signing a voluntary informed consent.
- Participants were treated equally and fairly throughout the research.

4.6 SUMMARY

This chapter outlined the research methodology used in the study. It provided a perspective on the research design process, outlining the research philosophy, research approach, and research strategies used in this study. It also outlined the three phases of the case study, as adapted from (Yin, 2003). Furthermore, the chapter described the data collection, analysis and validation techniques applied in the study. The next chapter presents the process of refining and validating the proposed ECISP Framework.

5. CHAPTER 5: REFINEMENT AND VALIDATION OF THE PROPOSED ECISP FRAMEWORK



5.1 INTRODUCTION

The previous chapter outlined the research methodology used to conduct the study. This chapter aims to refine and validate the conceptual ECISP Framework. This phase is defined as the *prepare, collect and analyse* step for a case study approach (Yin, 2003). The feedback acquired during the refinement and validation process is discussed and applied to refine and validate the conceptual framework. The feedback from government employees was used to answer the research question, SRQ 3: *What elements constitute a validated framework for end-user ISP compliance in a government institution?*

5.2 OVERVIEW OF CHAPTER 5

Chapter 5 begins with the refinement and validation process used in this study (section 5.3). This includes refining the conceptual framework through interviews with government officials, interpreting the findings and recommendations from those interviews, and presenting the refined framework based on those recommendations (section 5.3.1). This is followed by validating the refined ECISP Framework through expert interviews, interpreting the data obtained, and presenting the validated ECISP Framework based on recommendations from the validation process (section 5.3.2). Section 5.4 summarises the chapter.

5.2.1 STAGES OF REFINING AND VALIDATING THE FRAMEWORK

Table 5-1 outlines the stages of refining and validating the ECISP Framework.

Table 5-1 : *Stages of Refining and Validating the Framework*

Stage	Timeframe
Data collection: Collecting data through interviews to assess and confirm the conceptual ECISP Framework by government officials.	12 - 16 weeks
Transcribing and analysing the conceptual EISP compliance framework.	4 - 6 weeks
Review the framework: Using feedback from the interviews with government officials to refine the EISP compliance framework.	4 - 6 weeks
Data collection: Collecting data through interviews to validate the refined ECISP Framework by expert reviewers.	3 - 4 weeks
Transcribing, analysing and reporting: Analysing, interpreting, and summarising feedback acquired from experts.	4 - 6 weeks
Review the refined ECISP Framework: Using feedback from the expert reviews to improve the refined ECISP compliance framework.	4 - 6 weeks

The next sub-section discusses the refinement process followed to refine the conceptual ECISP Framework for government departments in South Africa.

5.3 FRAMEWORK REFINEMENT AND VALIDATION: APPLYING YIN'S CASE STUDY METHOD

This section provides an overview of the process for refining and validating the proposed conceptual ECISP Framework. The Yin (2003) case study approach was applied during the refinement and validation of the conceptual ECISP Framework.

5.3.1 FRAMEWORK REFINEMENT

The refinement process was conducted through demonstrations and interviews with government officials.

5.3.1.1 Findings from Interviews with Government Officials

The purpose of the refinement was to improve the conceptual ECISP Framework to ensure it addresses the needs of government institutions. This section outlines the feedback from the fourteen government officials interviewed. The responses were interpreted using the hermeneutic cycle to confirm the components and factors of the conceptual ECISP Framework. The hermeneutic cycle was considered suitable for this study because it applies a process of iterative interpretation. It supports that participants' responses be understood individually in relation to the overall context of the study (Creswell & Poth, 2016). The refinement of the framework through the use of participants' responses supported the refinement and validation of the ECISP framework.

5.3.1.1.1 Framework completeness

Government officials were asked to share their views on the completeness of the conceptual framework. As shown in **Figure 5-1**, codes derived from the interviews were categorised to confirm the completeness of the conceptual ECISP compliance framework. In **Figure 5-1**, the completeness of the framework was reviewed. The subsequent codes, as illustrated in the diagram, were derived from feedback from government officials.

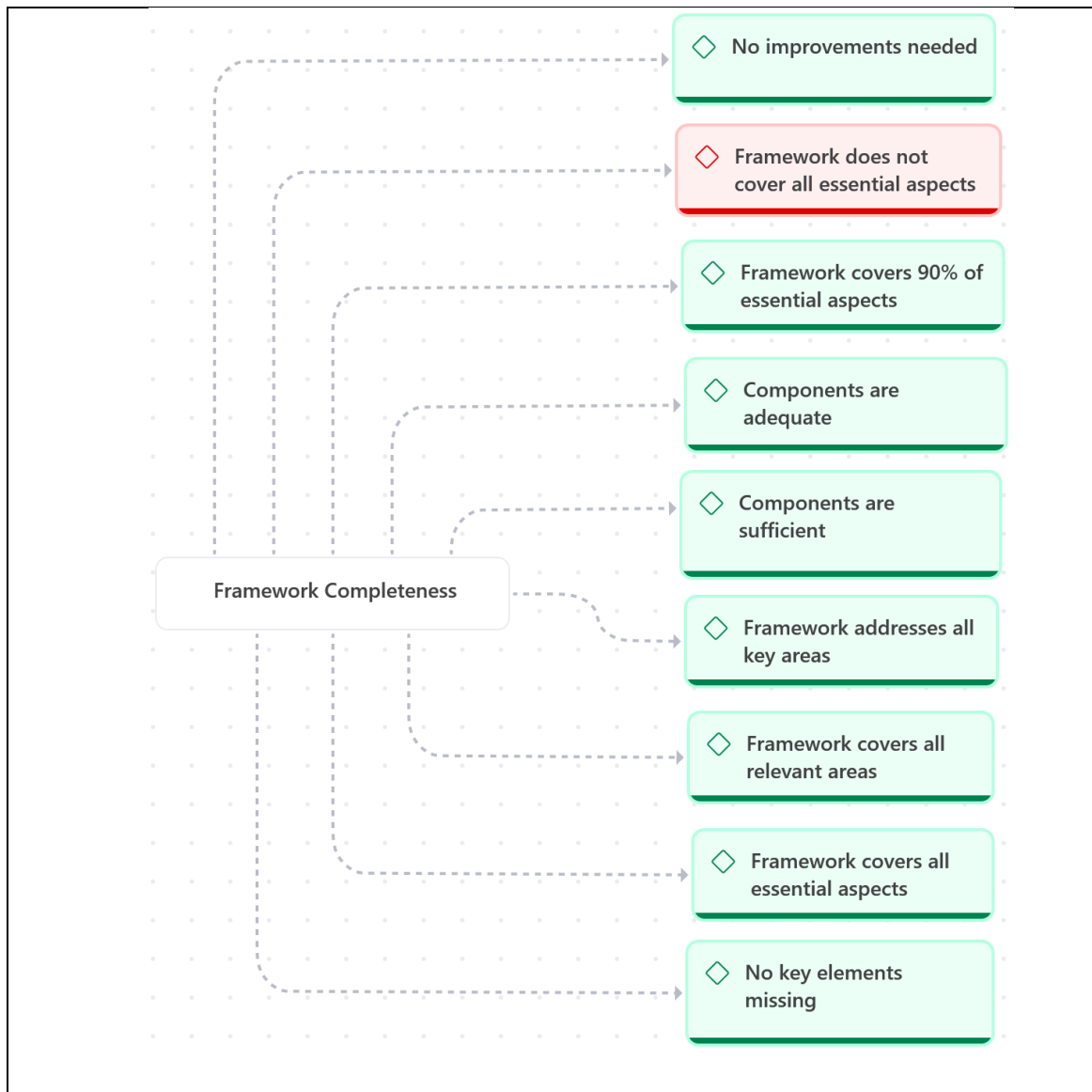


Figure 5-1: Completeness of the Framework - Thematic Diagram

Most participants, including Participants 1, 2, 5, 7, 8, 10, 11, 12, and 14, believed that the framework addresses all essential aspects. For instance, Participant 11 emphasised that the framework “*covers all important aspects that can assist the department to enhance end-user compliance with information security policy.*” Participant 8 stated, “*Yes, it does. I checked my information security procedure manual and compared it with the components of the framework, and many of the issues align.*”

Moreover, Participants 2, 5, 8, 9, 12, 13, and 14 stated that no key elements were missing from the framework. Participant 1 also mentioned that the components were “*sufficient.*” Participants 9 and 10 further mentioned that the framework covers all relevant areas.

Participant 3 offered a different perspective, suggesting that the framework covers about 90% of the essential aspects. She stated, *“I would say maybe 90% is covered because some of the aspects are identified as we continue implementing the policies.”* and *“I am saying it is 90% because there is always something new and we always have to do our research in terms of security, and we must always be at least a few steps ahead just to protect the organisation’s information from cybercrime.”* Participant 3’s feedback indicates that, although the framework is largely comprehensive, emerging information security challenges may require ongoing updates.

Although most participants confirmed the framework's completeness, Participant 4 offered a different view, indicating that it does not cover all essential aspects. He stated, *“No, the framework does not cover enforcement and the consequences for non-compliance, such as disciplinary actions or penalties for individuals who fail to comply with the information security policy.”* This feedback suggests that the framework should be improved to include enforcement mechanisms for information security policy compliance.

Contrarily, Participants 5, 12, and 14 stated that no improvements are required, highlighting that the framework is complete and effective as is.

5.3.1.1.2 Suitability of the framework

Participants were asked to share their views on the framework’s suitability. This process demonstrated consensus among participants regarding the framework’s alignment with the needs and challenges of government institutions as depicted in **Figure 5-2**.

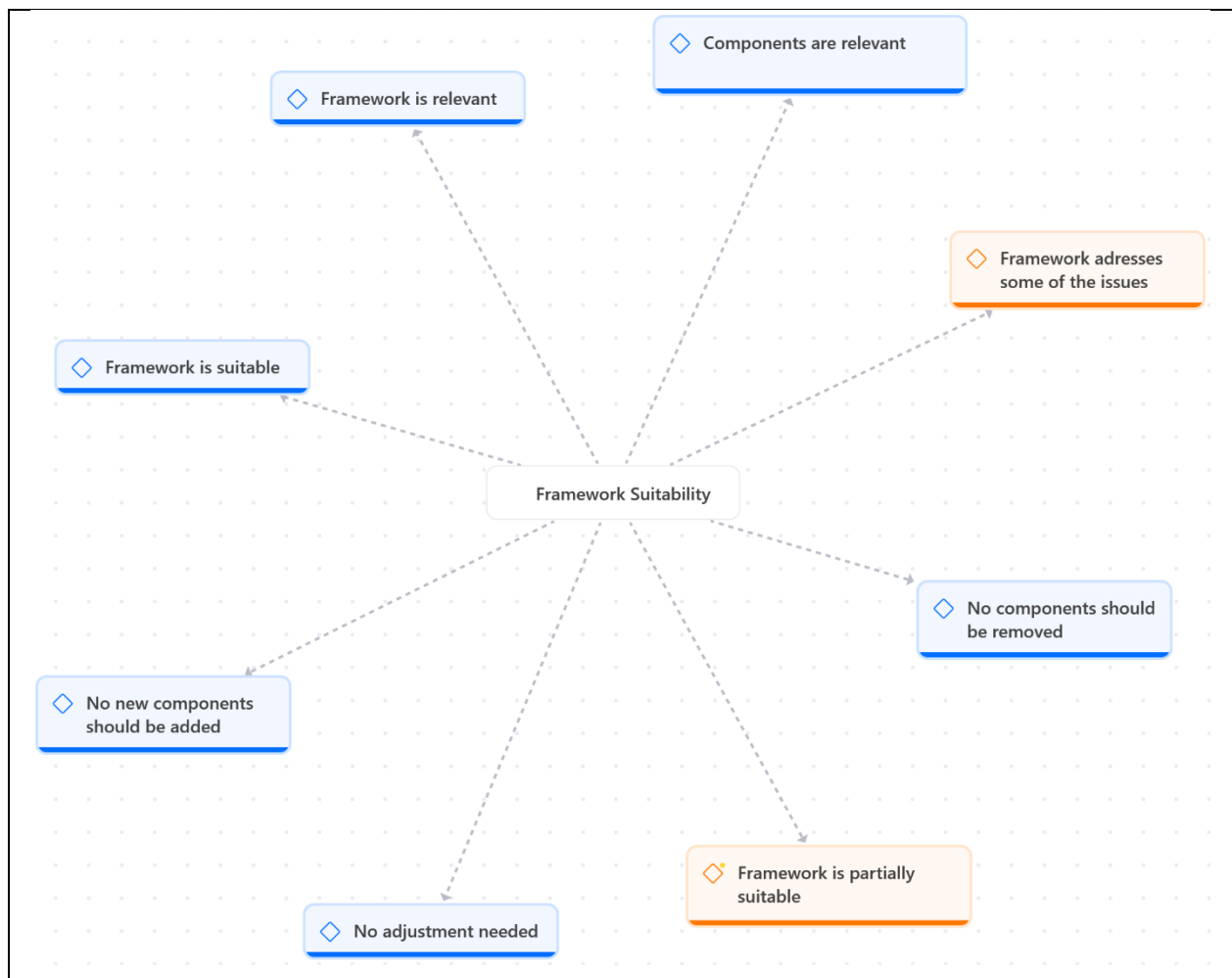


Figure 5-2: Suitability of the Framework - Thematic Network Diagram

Most participants stated that the framework's components are relevant, with Participants 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 12, and 14 confirming this.

Most participants confirmed that the framework was suitable for their organisations. Participants 1, 2, 4, 5, 7, 8, 10, 11, and 12 agreed that the framework was suitable. Participant 12 stated, *“Yes, I think the framework is suitable for my organisation as it consists of factors and components that are relevant to the challenges in our organisation.”* However, Participant 13 partially agreed with the framework’s suitability, noting that while it is largely suitable, influencing individual personalities and beliefs in the workplace can be challenging, and stated: *“I partially agree that the framework is suitable for our institution's needs. However, influencing individual personalities and beliefs within a workplace setting can be challenging.”* Similarly, Participant 14 stated that the framework addresses some of the issues affecting compliance with ISP.

Several participants believed the framework is suitable as it stands and requires no additional components. Participants 1, 3, 5, 9, 10, and 11 stated that no new components should be added. In addition, the majority agreed that none of the existing components should be removed. Participants 3, 4, 5, 6, 7, 9, 11, 12, and 13 emphasised that all components are essential and should remain intact.

When asked about potential adjustments to the framework, many participants stated that no changes were needed. Participants 5, 8, 10, 11, 12, 13, and 14 believed the framework was well-structured and effective in addressing compliance challenges in its current form.

5.3.1.1.3 Applicability of the Framework

The government officials were asked to evaluate the applicability of the framework. The evaluation of the framework's applicability focused on assessing whether the components and the framework as a whole can be effectively applied in government institutions. As shown in **Figure 5-3**, codes derived from the interviews, based on participants' responses, were categorised to evaluate the applicability of the ECISP Framework. Participants offered different views on the applicability of the conceptual ECISP Framework.

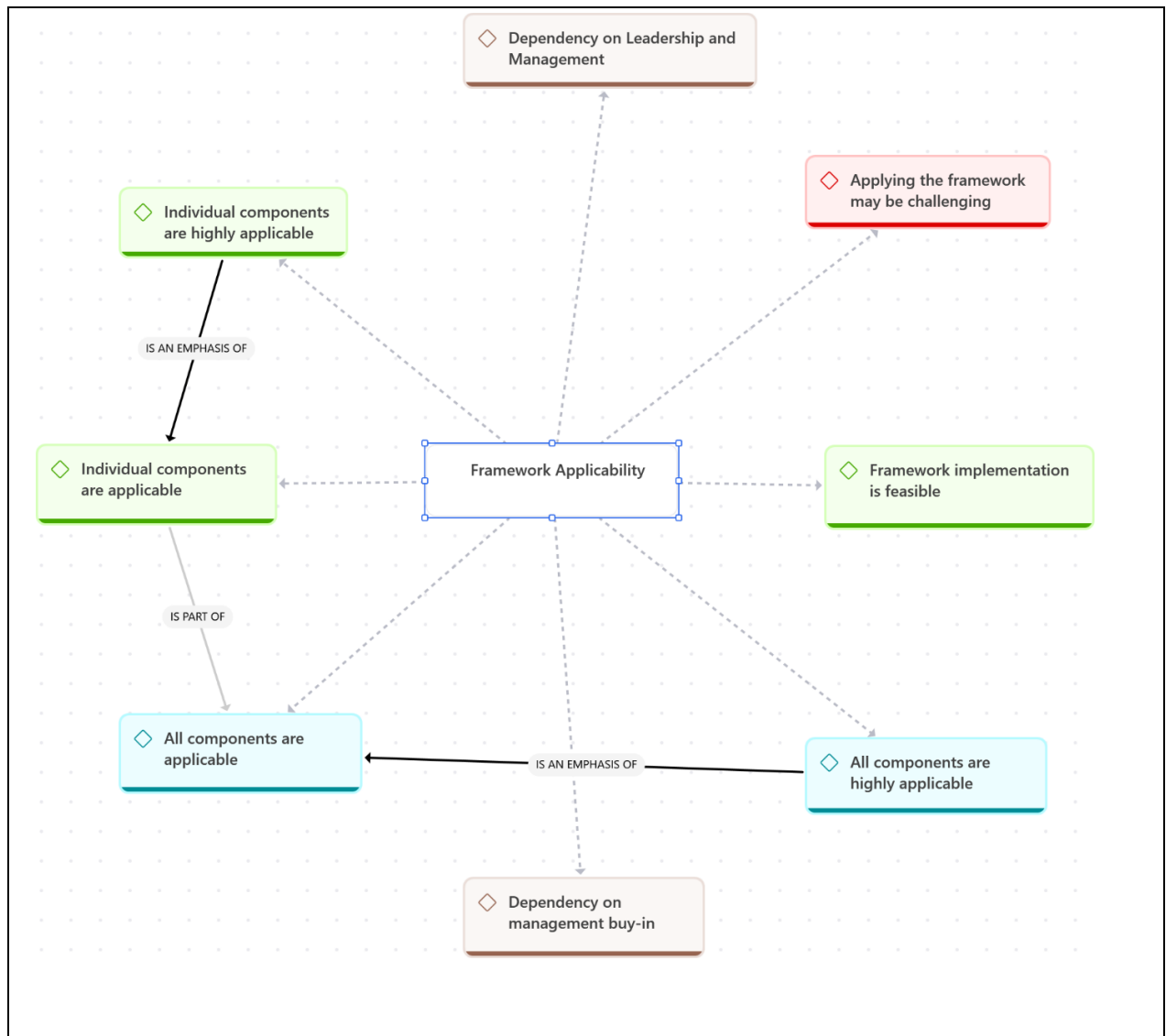


Figure 5-3: Applicability of the Framework - Thematic Network Diagram

Participants 1, 2, 3, 4, 6, 8, 9, 10, and 12 indicated that the components are applicable to their organisational contexts. Furthermore, Participants 5 and 14 mentioned that the components are highly applicable. However, some participants noted that leadership and management effectiveness depend on the framework's applicability. Participants 8, 13, and 14 mentioned that management plays an important role in ensuring the framework's successful implementation.

Participant 13 stated, *"I would say if the framework can be implemented by supervisors, everyone in the organisation has a supervisor. So, if it's implemented by the supervisors, it will be easy for others to follow."* Similarly, Participant 14 stated, *"It will depend on the leadership and the management to ensure that it is implemented; they play a very critical role in order to*

ensure we see it implemented as proposed, it is possible to achieve.” Participant 8 shared the same sentiment and stated that, “This starts again from the management part; management should come to the space and ensure that officials are held accountable to anything that they're doing. If management takes the lead, I believe it would be easy to implement the framework as it's proposed.”

Regarding the individual components of the conceptual framework, Participant 11 agreed they are applicable, while Participant 13 stated they are highly applicable. This feedback suggests that the components align with the needs of government institutions for ISP compliance.

Most participants also believed that implementing the EISP compliance framework is feasible. Participants 1, 2, 3, 4, 5, 8, 9, 10, 11, 12, and 13 believed that the framework could be introduced into their organisations. Participant 11 stated, *“I think the feasibility of implementing it depends on management buy-in.”*

Participants 6 and 7 mentioned possible challenges in implementing the framework. Participant 6 stated, *“Some of the controls in terms of these components require resources. It's not because people don't want to comply, it's because we don't have resources such as financial resources, human resources and working tools like equipment and computers. Some people are sharing equipment, which makes it difficult to comply with some of the ISP requirements. So, the framework can be easy to apply if resources are made available.”*

Participant 7 also stated, *“Applying it in the organisation might be challenging. It will depend on whether the leadership and management of the department adopt and implement the framework. Even if it might be easy to use, implementation might not be easy.”* These observations and feedback show the importance of leadership commitment and addressing resource constraints to enhance the framework's applicability.

5.3.1.1.4 Usability of the Framework

Government officials were asked to confirm the framework's usability. The confirmation of the framework's usability focused on verifying whether the components and the framework as a whole are easy to use and apply within government institutions. As outlined in **Figure 5-4**, the codes derived from the interviews were categorised to verify the usability of the conceptual ECISP Framework

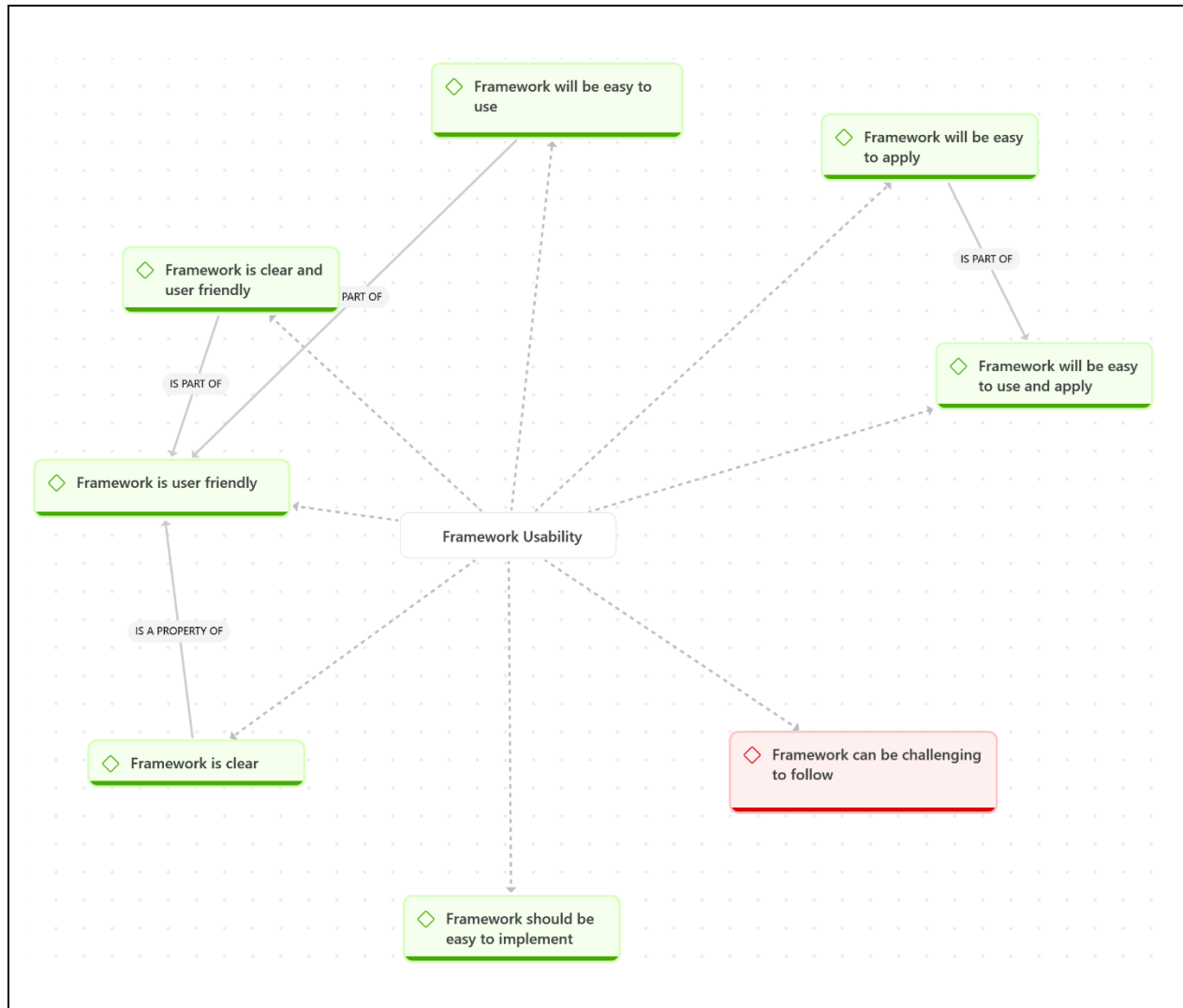


Figure 5-4: Usability of the Framework - Thematic Network Diagram

Most participants stated that the conceptual framework is clear, user-friendly, and straightforward to apply in their organisations. Participants 6 and 7 stated that the framework would be easy to use. Likewise, Participants 1, 11, 12, and 13 shared the same sentiments, stating that the framework would be easy to apply in their organisations. Furthermore, Participants 2, 3, 8, 11, 12, and 14 stated that the framework would be both easy to use and apply.

Participants 4, 9, 10, and 11 stated that the framework is clear and straightforward. Participant 1 stated, *“I think it is user-friendly because it speaks to the basic things that influence end-user behaviour.”* In addition, Participants 5, 8, 12, and 14 shared the same sentiment, with Participant 5 stating, *“The framework is very clear and user-friendly. I do not see any area that requires improvement.”*

Although the overall feedback was positive, Participant 2 highlighted concerns regarding potential challenges in following the framework. He stated, *“The framework can be a bit challenging to follow. However, breaking it down into procedural steps and addressing specific areas will improve its clarity and overall understanding for end users.”* This feedback identifies a gap and highlights the need for procedural guidance to ensure end-user adoption. Participant 9 stated that the framework would be easy to implement in their organisation.

5.3.1.1.5 Most Suitable and Relevant Components and Factors

Participants were also asked to identify the components of the framework they consider most suitable and relevant for enhancing end-user compliance with information security policies in government institutions. This verification was conducted to determine which aspects of the framework align with the participants’ practical experiences and organisational needs. **Figure 5-5** presents the outcome of the participants’ responses on the factors and components’ suitability and relevance.

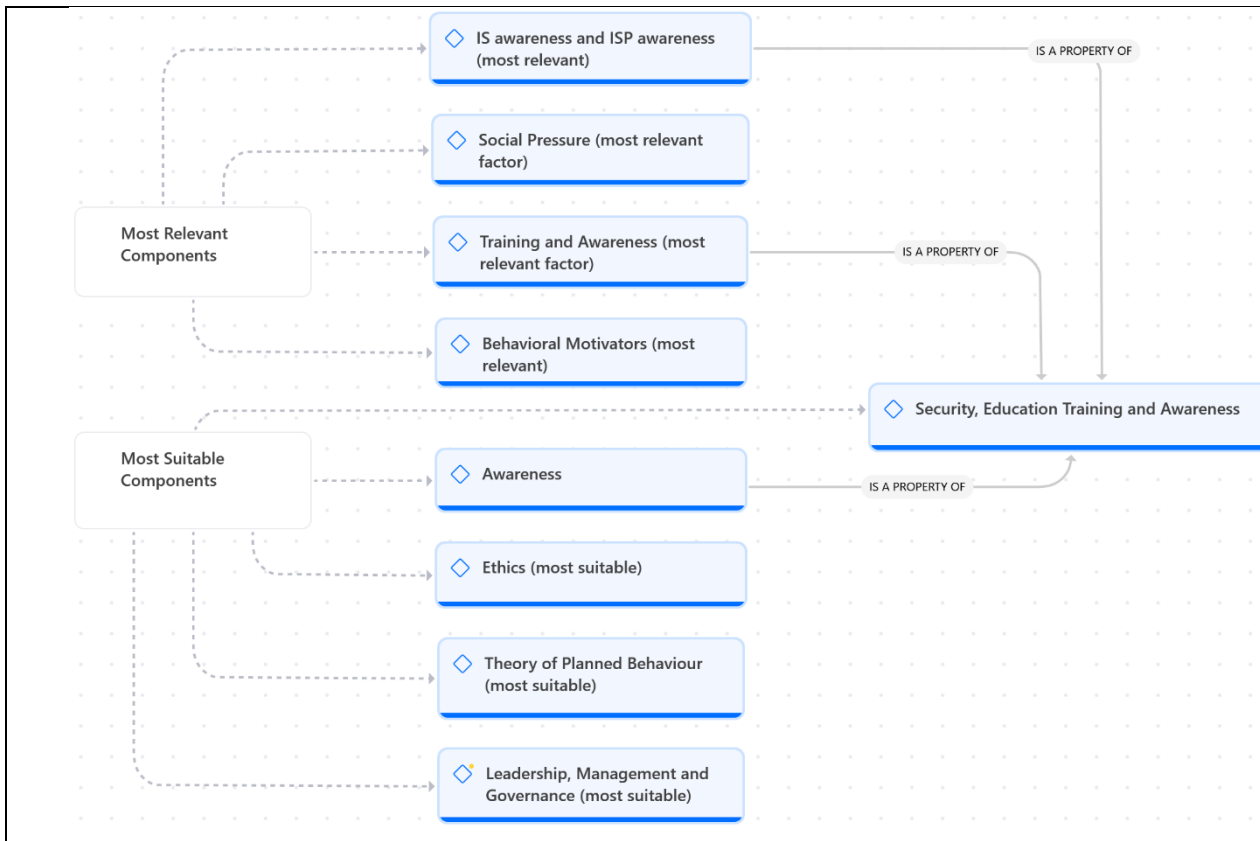


Figure 5-5: Most Suitable and Relevant Components and Factors - Thematic Network Diagram

As shown in **Figure 5-5**, the codes derived from the interviews were categorised to verify the conceptual ECISP Framework and identify the most suitable and relevant components. Two themes were used to represent the most suitable and relevant components as identified by the participants. The relationship between the suitability and relevance of components and factors was illustrated in a single network diagram. This interconnected representation highlights how participants' responses/identified factors and components are linked between the two themes.

Participants were asked to select the most suitable and relevant components of the conceptual ECISP Framework for enhancing end-user compliance with information security policies. Although the question focused on components, some participants also mentioned specific factors within them. This suggests that certain components' factors were deemed key to enhancing their organisation's end-user compliance with ISP.

Regarding the most relevant components and factors, participants identified key areas they believed were essential to improving end-user compliance with ISP in their organisations. Participants 5 and 9 identified behavioural motivators as the most suitable. Participant 4 identified social pressure as an important factor. Training and awareness were also identified. Participant 4 identified them as relevant factors, and Participants 5, 7, 11, and 13 identified

security education, training, and awareness as important components. Although training and awareness were deemed important components, their related factors, such as security education and IS awareness, were specifically mentioned by Participant 3 as directly relevant to participants' experiences and organisational needs.

Leadership, management, and governance were frequently mentioned as the most suitable components and factors. Participants 4, 6, 7, 8, 9, 12, and 14 highlighted their importance. Participant 1 identified ethics as the most suitable component.

5.3.1.1.6 Proposed new components and factors

Participants were asked to indicate whether they would add or propose new components or factors to the conceptual ECISP Framework. **Figure 5-6** presents the results of the coding based on the participants' responses on proposing new factors and components to the conceptual ECISP framework.

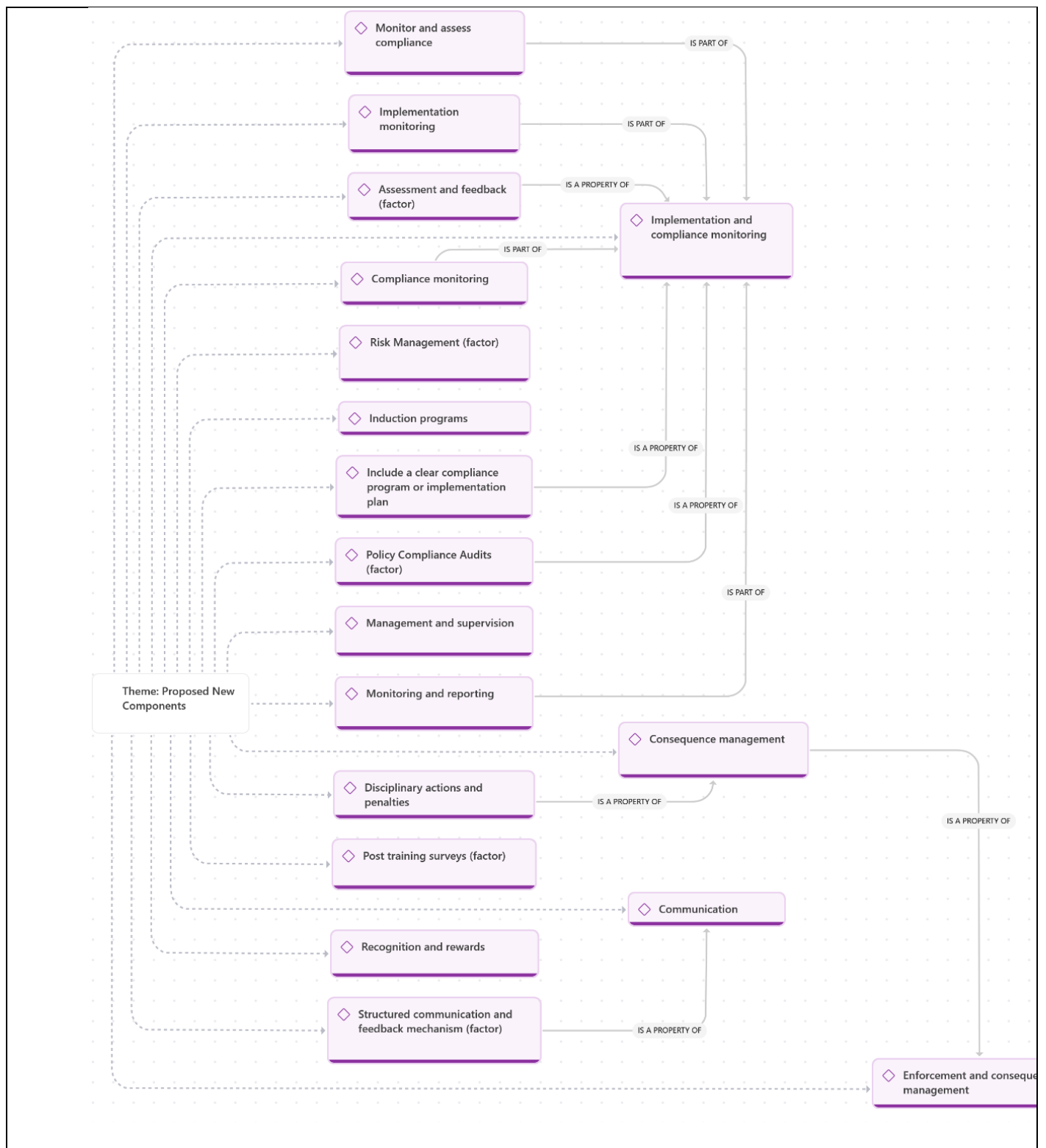


Figure 5-6: Proposed New Components and Factors - Thematic Network Diagram

As shown in **Figure 5-6**, the feedback presents a mix of proposed components and factors. Factors were the dominant additions, indicating participants' perceptions of areas in the conceptual framework that should be strengthened to enhance their organisations' end-user compliance with ISP.

Participant 6 proposed adding components such as conflict-of-interest management, resource allocation for compliance, a consequence management system and structured communication and feedback, stating that *“There should be a structured approach to ensure that information reaches every employee and includes a feedback mechanism. This would allow us to monitor any progress and develop continuous improvement strategies based on the feedback received.”*

Likewise, Participant 4 proposed factors to enhance implementation and accountability, including post-training surveys; enforcement and consequence management; tailored training; implementation monitoring; inclusion of IS compliance in induction programmes; policy compliance audits; and assessment and feedback mechanisms.

Participant 13 proposed the inclusion of a clear compliance programme or implementation plan, monitoring and reporting mechanisms, and a recognition and rewards system to improve end-user compliance with ISP. He stated, *“I believe that including a clear compliance programme to the framework would be beneficial. It should outline the steps needed to encourage and ensure compliance with the policy. A compliance programme booklet or implementation plan could be useful, detailing what actions need to be taken to effectively comply with ISP.”*

Participant 9 suggested adding compliance monitoring and assessment as factors. Similarly, Participant 7 proposed an implementation and compliance-monitoring component, the inclusion of ISP compliance in induction programmes, and management and supervision as additional components and factors within the proposed ECISP compliance framework. Finally, Participant 2 proposed the inclusion of a recognition-and-rewards system to promote end-user compliance with information security policies.

5.3.1.2 Refined ECISP Framework

The results of interviews with government officials informed the refinement of the conceptual ECISP Framework. Participants also provided recommendations for additional components and factors. These recommendations were assessed and incorporated into the framework to improve its applicability, usability, completeness, and relevance.

The recommendations included adding an implementation and compliance monitoring component to the refined ECISP Framework, with proposed factors such as policy compliance

audits, compliance monitoring, assessment and feedback, and a compliance implementation plan. Other proposed factors were reviewed, aligned, and assigned to appropriate components within the framework. These include conflict-of-interest management, resource allocation for compliance, consequence management, integrating ISP compliance awareness into induction programmes, post-training surveys, and the inclusion of recognition and reward systems to incentivise compliance. These updates ensure that the framework is better aligned with the operational realities and motivational drivers within government institutions, making it more robust and user centred.

Figure 5-7 presents the revised framework diagram, incorporating the proposed refinements from government officials. The proposed factors and components derived from thematic analysis of the government official interviews are indicated by asterisks (*) next to them as bullet points, while the initial components are shown with standard bullet points.

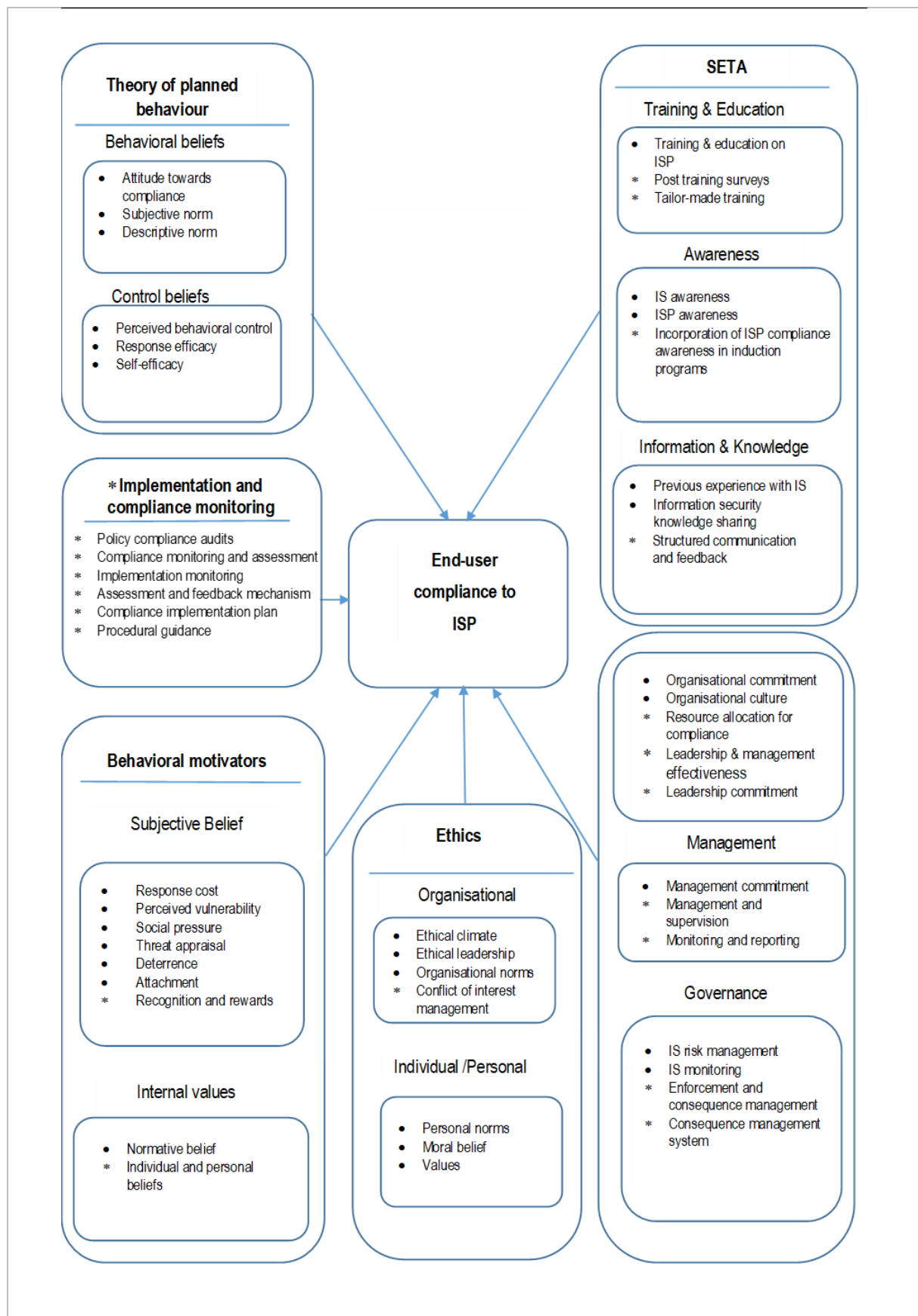


Figure 5-7: The Refined Framework

Following the refinement process, the refined framework was demonstrated to and validated by subject-matter experts. The updated components were also demonstrated to the experts, and interview questions focused on assessing the framework's accuracy, comprehensiveness, relevance, and effectiveness. This validation process confirmed the framework's accuracy and applicability across government settings.

5.3.2.1 Findings from Interviews with Information Security Experts

The demonstration and validation phase enhances the quality and credibility of the research results and addresses the knowledge gap by ensuring the proposed ECISP Framework is thoroughly validated through expert feedback.

This section presents feedback from the four information security experts. The responses were interpreted using the hermeneutic cycle to validate the components and factors of the refined ECISP compliance framework. The sections below outline the results of the data analysis for the themes developed.

5.3.2.1.1 Framework Accuracy

The information security experts were asked to provide their views on the framework's accuracy. **Figure 5-8** presents the results of the coding and themes based on the responses from the experts of the refined ECISP framework's accuracy.

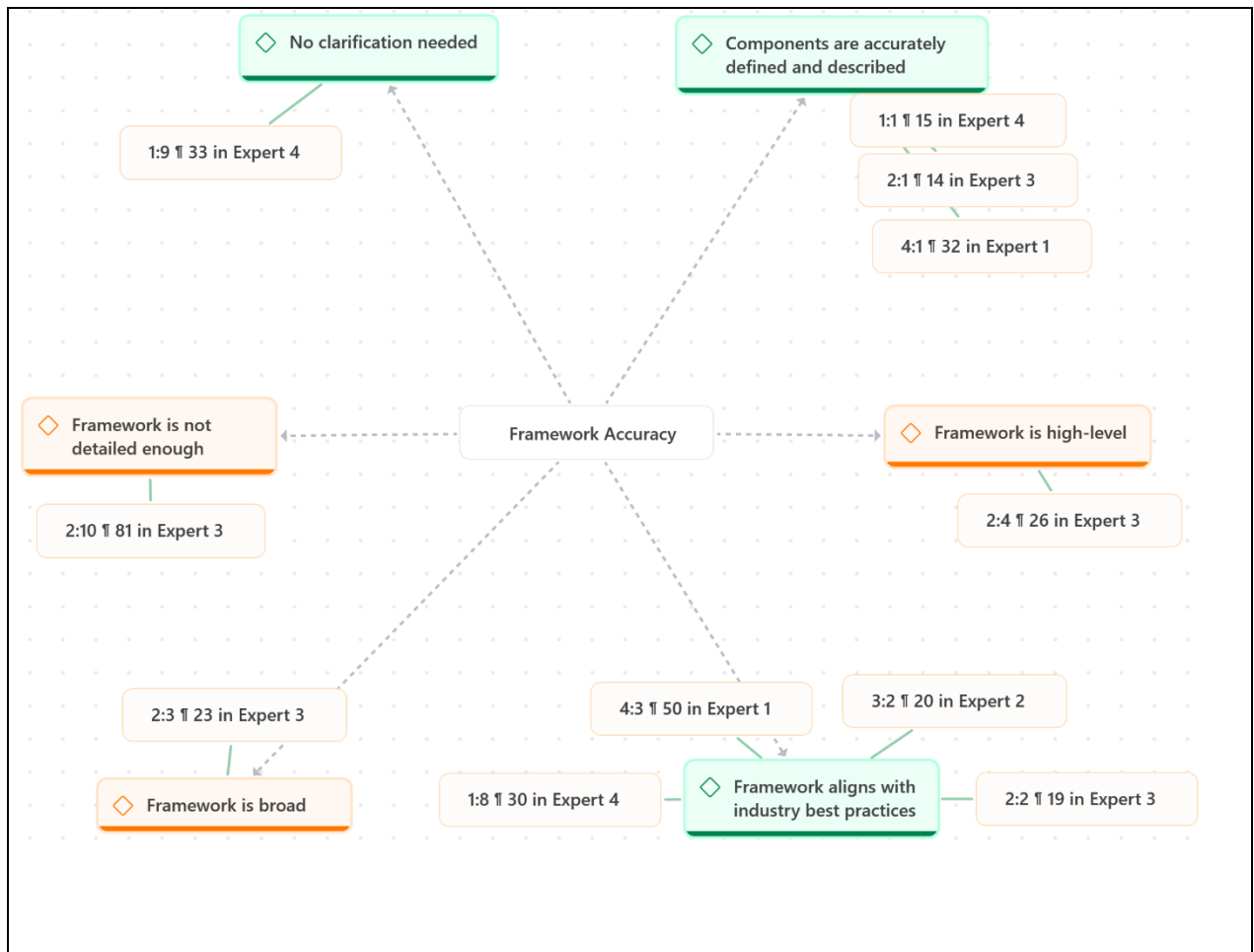


Figure 5-8: Framework Accuracy - Thematic Network Diagram

As shown in **Figure 5-8**, the codes derived from the interview were developed based on expert feedback and categorised to validate the accuracy of the refined ECISP Framework.

Three of the four experts confirmed that the components are accurately defined and described. Expert 4 further stated that no clarification is needed. In addition, all four experts believed that the framework aligns with industry best practices. Expert 4 stated, “*The components that you have developed are in line with standards, the main one being ISO 27 001.*” This alignment supports the framework’s link with international information security standards. While the ISO 27001 focuses on technical security controls, the ECISP focuses on end-user compliance to ISP. Expert 3 offered a different view, noting that the framework is high-level, broad, and not detailed enough. Expert 3 stated, “*The only issue with this framework is that it is very high level, and it does not have enough information there to say whether it is sufficient. When you look generally at frameworks, it has some steps in there that you must do.*”

5.3.2.1.2 Framework Comprehensiveness

The experts were asked to assess the comprehensiveness of the refined ECISP Framework. Validating comprehensiveness is important to ensure that the ECISP Framework covers all key aspects required to enhance end-user compliance with the ISP. **Figure 5-9** presents the results of the coding and themes based on the experts' responses on the refined ECISP framework's comprehensiveness.

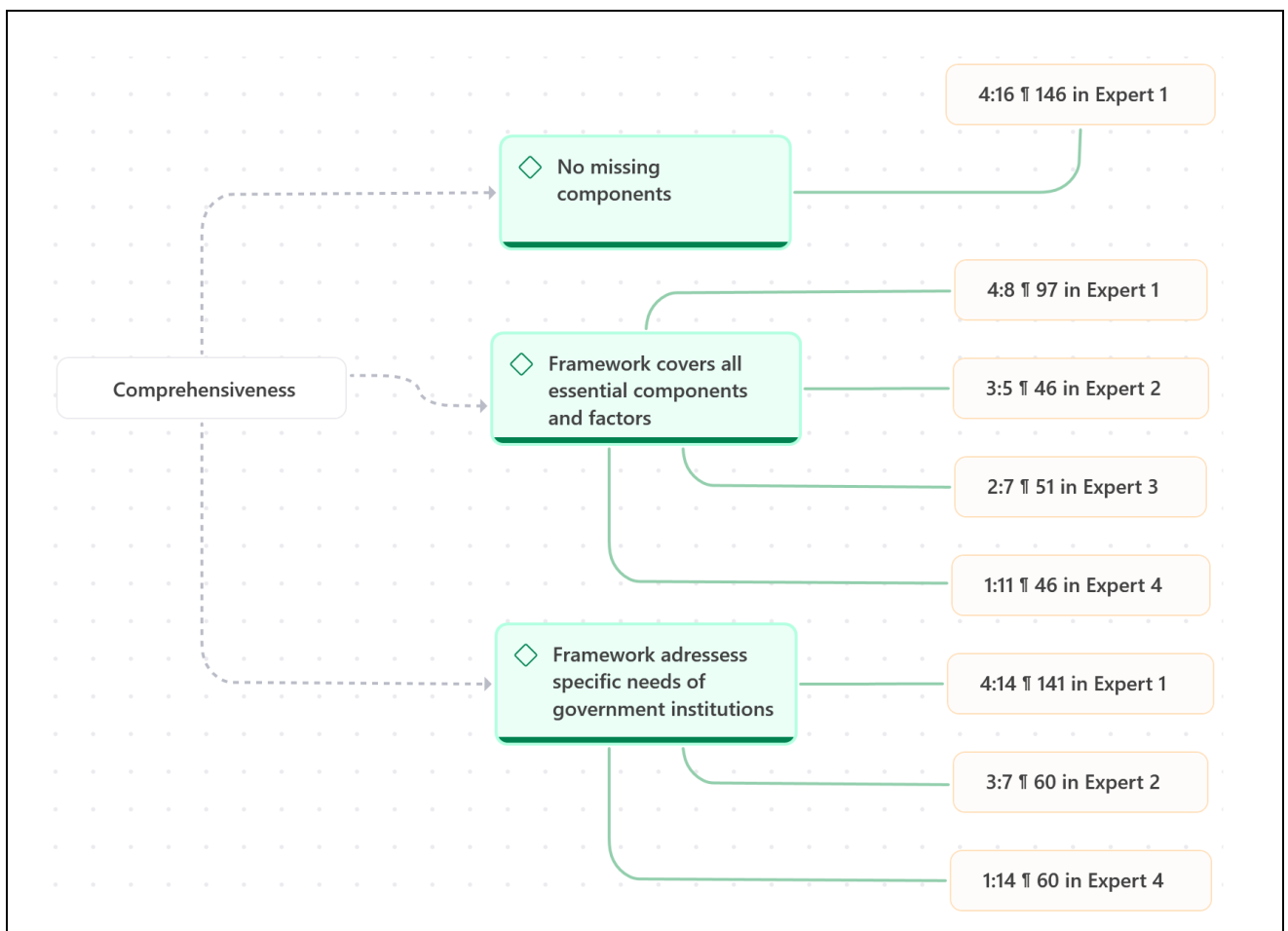


Figure 5-9: Framework Comprehensiveness - Thematic Network Diagram

The feedback indicates that the experts agreed that the refined ECISP Framework is comprehensive. All experts indicated that the framework covers all essential components and factors. Furthermore, Experts 1, 2, and 4 noted that the framework addresses the specific needs of government institutions. Expert 4 stated that *“The framework addresses the specific needs. If anything, I think it addresses most of the issues that are common in most government departments.”*

5.3.2.1.3 Framework Relevancy

Experts were asked to assess the framework's relevance. This section focuses on validating whether the framework addresses government departments' unique challenges, is adaptable to potential changes, and whether the framework as a whole is relevant. **Figure 5-10** presents the results of the coding and themes based on the experts' responses on the refined ECISP framework's relevancy.

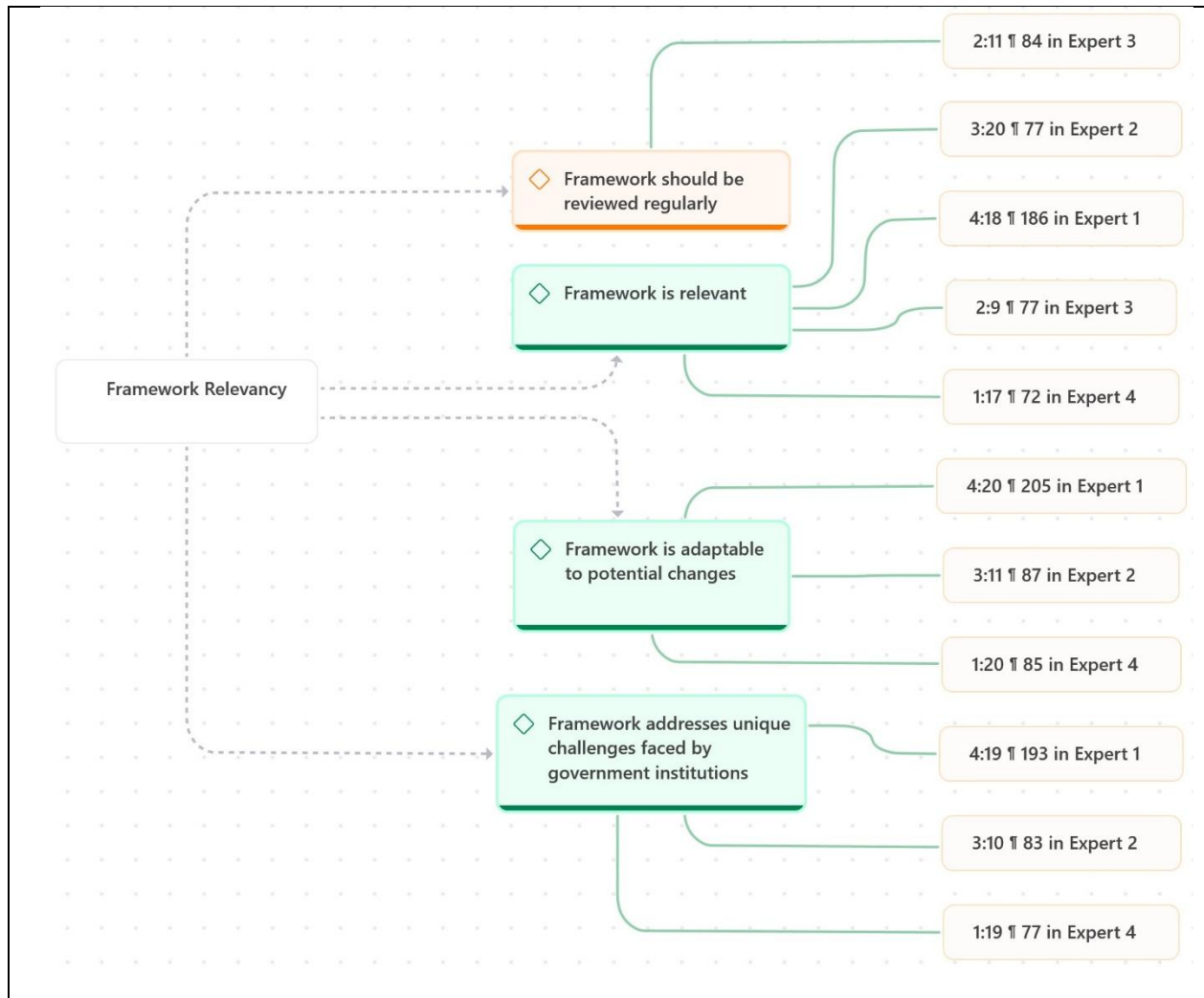


Figure 5-10: Framework Relevancy - Thematic Network Diagram

As shown in **Figure 5-10**, the codes derived from the interviews were categorised to validate the framework's relevance. Most experts indicated that the framework is relevant and addresses the unique challenges faced by government institutions. Experts 1, 2, and 3 stated that the framework is relevant. Furthermore, experts 1, 2, and 4 stated that the framework addresses the unique challenges faced by government institutions. Expert 2 stated that *"The framework addresses unique challenges of government institutions, especially the issue of awareness and training, consequence management, and compliance audits."* Similarly, Expert 1 shared the

same sentiments and stated that *“Particularly in relation to the SETA component, one challenge in government departments is that they focus on awareness rather than providing comprehensive information security training for end-users.”*

Additionally, Experts 1, 2 and 4 confirmed that the framework is adaptable to potential changes, meaning it can be amended as and when required to align with emerging policies and operational needs. Expert 1 stated that *“This framework is applicable to both traditional and hybrid work environments, because issues of end-user behaviour focus on how the employee views and reacts on issues related to information security, whether working in the office or remotely.”*

Although most experts agreed that the framework is adaptable, Expert 3 expressed a different view, stating that frameworks must be regularly reviewed to align with changes in the environment. *“Frameworks are always going to be changed and adaptable, if you understand that periodically they need to be updated and reviewed because technology changes.”*

5.3.2.1.4 Framework Effectiveness

Experts were asked to validate the framework's effectiveness and assess whether it would enhance end-user compliance with ISP requirements in government institutions. **Figure 5-11** presents results of the coding and themes based on the experts' responses on the refined ECISP framework's effectiveness.

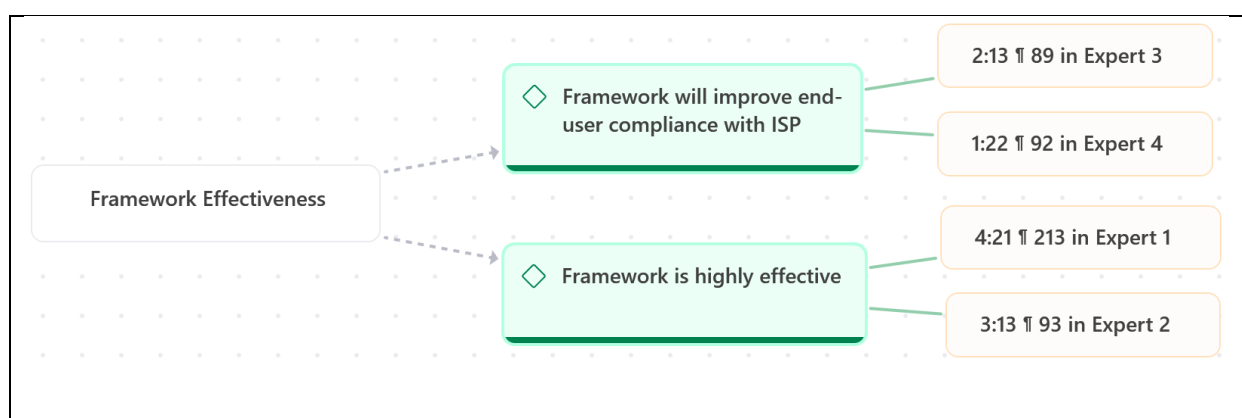


Figure 5-11: Framework Effectiveness - Thematic Network Diagram

As shown in **Figure 5-11**, the codes derived from the interviews were used to validate the framework's effectiveness. The experts shared similar views and indicated that the framework is effective. Experts 1 and 2 stated that the framework is highly effective, while Experts 3 and

4 agreed that the framework will improve end-user compliance with the ISP. This feedback confirms that the framework has the potential to enhance end-user compliance with the ISP within government departments.

5.3.2.1.5 Most Contributing Components

Experts were also asked to identify the components of the framework they believed contributes the most to enhancing end-user compliance with ISP. This was done to identify the components of the framework they considered most important for enhancing end-user compliance with ISP. **Figure 5-12** presents the results of the coding and themes based on the experts' responses on the components they believed contributes the most to enhancing end-user compliance with ISP.

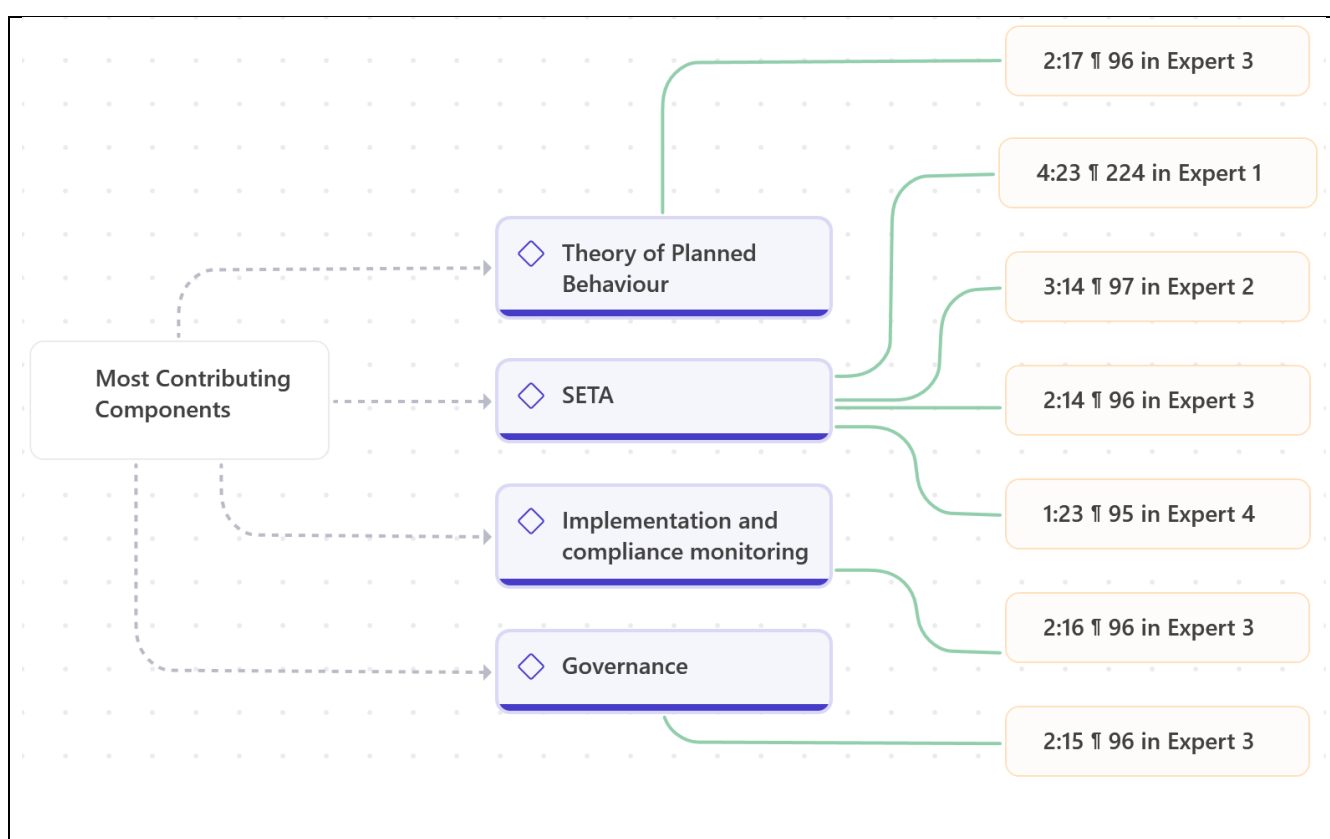


Figure 5-12: Most Contributing Components - Thematic Network Diagram

As shown in **Figure 5-12**, the codes derived from the interviews were used to validate the framework and identify the most significant components. Expert 3 mentioned the theory of planned behaviour, implementation and compliance monitoring, SETA and governance. In addition, Experts 1, 2, and 3 confirmed that SETA is the primary contributor to enhancing end-user compliance with ISP within government departments. A similar view from experts indicates the importance of focusing on training and awareness as key components for improving compliance behaviour across departments.

5.3.2.1.6 Proposed Additional Components

The experts were asked to indicate whether any aspects of the refined ECISP Framework were missing or whether any areas might benefit from improvement. They were also asked to suggest any additions they believed could improve end-user compliance with information ISP within government departments. **Figure 5-13** presents results of the coding and themes based on the experts' responses on the proposed addition components of the refined ECISP framework.

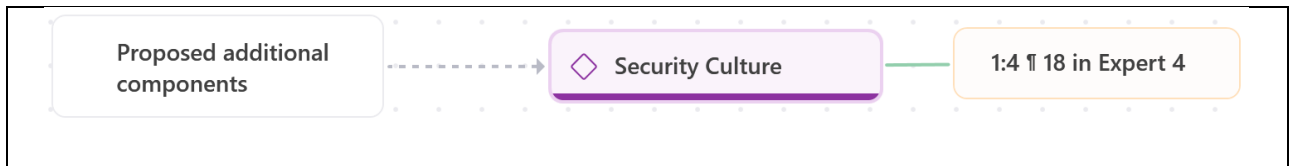


Figure 5-13: Proposed Additional Components - Thematic Network Diagram

As shown in **Figure 5-13**, only Expert 4 proposed adding a new component to the refined ECISP Framework and suggested that security culture be considered an additional component. He indicated that *“In awareness lately they speak about the culture of the organisation. I think the culture of security in departments is spilling out as well, that must change. The latest language now is moving away from awareness to culture behaviour in as far as security is concerned. I would take it as a separate component, although it is a new thing that the industry is trying to push. If you still want to add sub-components, perhaps you can look at the security culture and see how you can fit it under awareness.”*

5.3.2.1.7 Proposed Additional Factors

In addition to proposing new components, some experts proposed adding factors that could be integrated into the existing components of the refined ECISP Framework. **Figure 5-14** presents the results of the coding and themes based on the experts' responses on the proposed additional factors of the refined ECISP framework.

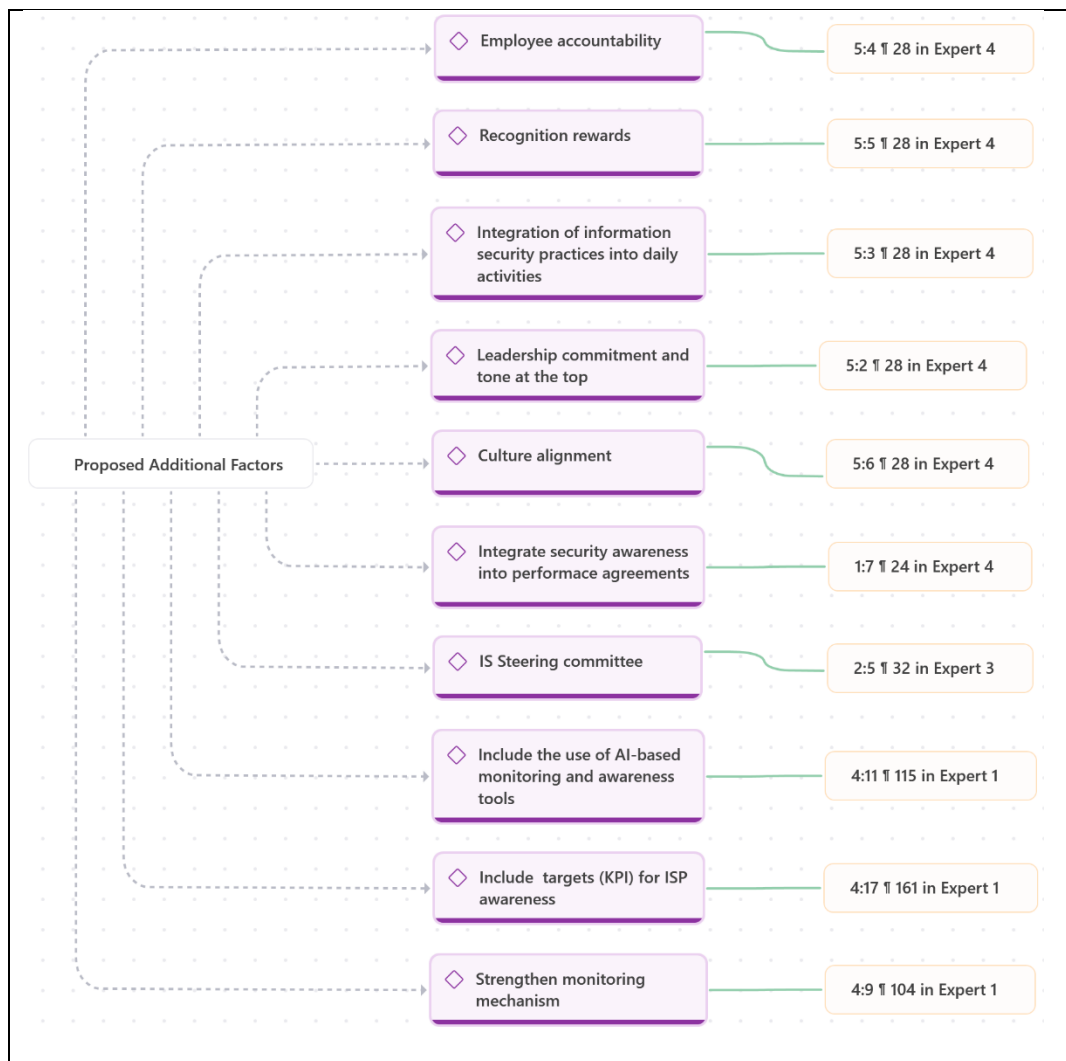


Figure 5-14: Proposed Additional Factors - Thematic Network Diagram

As shown in **Figure 5-14**, Expert 1 recommended incorporating AI-based monitoring and awareness mechanisms. He stated that *“If AI-based tools can be integrated into the framework, they could help enhance end-user behaviour. These tools would generate alerts for administrators and could even help them write compliance reports.”* He further proposed including key performance indicators (KPIs) for ISP awareness, stating, *“The framework should include metrics for evaluating compliance. Setting up KPIs for employees to complete phishing awareness training annually would provide a structured way to measure and improve security awareness.”* Expert 1 also recommended adding *“strengthening of monitoring mechanisms”* to enhance ongoing compliance efforts, by noting that *“I think the monitoring mechanism could be further enhanced. Strengthening the monitoring system could improve compliance. For example, organisations can implement tools like real-time dashboards to track compliance metrics”*.

Expert 3 suggested establishing an Information Security (IS) Steering Committee within the ECSIP framework. Expert 4 proposed adding another factor, “*integrating security awareness objectives into employees' performance agreements*”, to ensure that ISP compliance becomes part of employee performance assessments. He stated that “*The DPSA directive on information security indicates that security awareness should be integrated into officials' performance agreements, not just to inform them about security practices, but to create a cultural shift within the organisation.*”

Expert 4 also recommended including various factors in his proposed component on information security culture. He recommended adding leadership commitment and tone at the top as factors within information security culture, stating that “*Executive managers lead by example, model secure behaviour and communicate its importance to employees.*” He also recommended including a factor “*integration of information security practices into daily activities*” and indicated that “*security practices should be part of the day-to-day processes of an organisation*”. Furthermore, Expert 4 proposed employee accountability and stated that “*employees must be encouraged to report incidents without fear of punishment*”. He further proposed recognition awards and pointed out that “*organisations should acknowledge secure behaviours*”. Additionally, he proposed culture alignment and stated “*aligning security initiatives with the broader organisational culture and values.*” These additional factors highlight the importance of leadership involvement, technological support, and the formal embedding of security practices into organisational processes.

5.3.2.1.8 Proposed Framework Adjustments

Experts were also asked whether any areas within the framework required clarification or refinement to improve accuracy, and whether they had any comments on how the framework could be improved. **Figure 5-15** presents the results of the coding and themes based on the experts’ responses on the proposed framework.

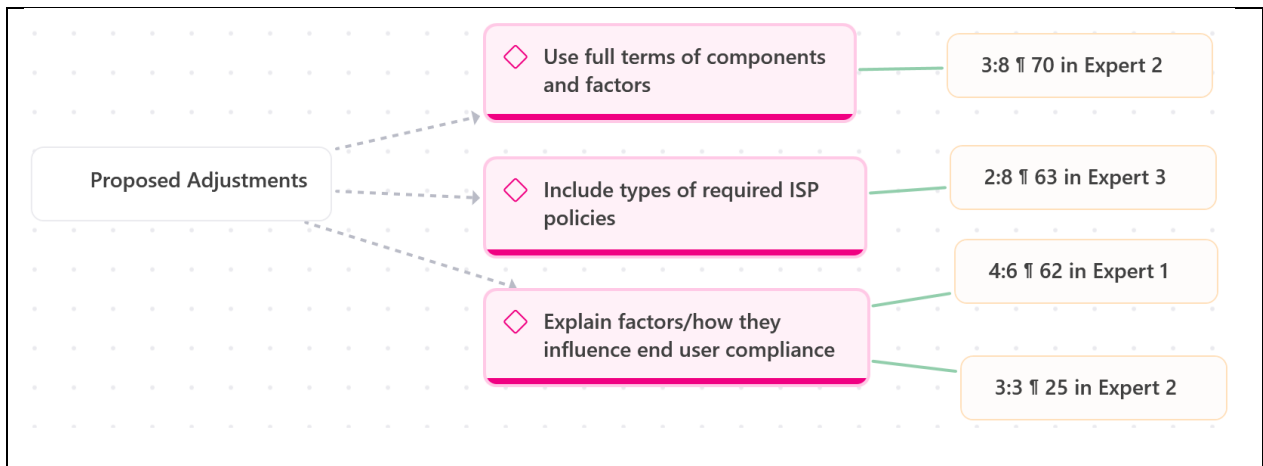


Figure 5-15: Proposed Framework Adjustments - Thematic Network Diagram

As outlined in **Figure 5-15**, Expert 2 recommended that the full terms for each component and factor be clearly stated rather than abbreviated.

Expert 3 proposed that the framework should include a list of the types of ISPs that organisations are expected to develop and enforce. She stated that *“You will find that people may have a policy, and all policies are understood, but a person may have an information security policy that does not have anything that speaks to acceptable use. So, when you have a framework, it guides the type of policies that are actually required by organisations to have. Everybody may have one policy, but they may be missing one or two policies here or there.”*

Additionally, both Expert 1 and Expert 2 recommended that the framework's factors be explained to help users, especially those without a strong background in information security, understand how they can be used to influence end-user compliance with ISP, thereby enabling the framework to be interpreted and applied in practice. Expert 1 stated, *“Some factors may not be easily understood by individuals outside the domains of information security policy compliance and user behaviour. For instance, response cost might be interpreted differently by different people. I recommend that the factors be clearly explained to ensure the intended reader understands them and interprets them within the correct context.”* Expert 2 shared the same sentiments and stated, *“I think it would be helpful to explain some of the terms, especially the factors, to make it easier for people to understand, explaining how they can influence end-user compliance.”*

5.3.2.1.9 Potential Challenges and Limitations

Experts were asked to share any potential challenges or limitations, based on their professional experience, that might affect the effectiveness of the refined ECISP Framework in enhancing end-user compliance with ISP. **Figure 5-16** presents the results of the coding and themes based on the experts' responses on potential challenges and limitations that may affect the refined ECISP framework's effectiveness.

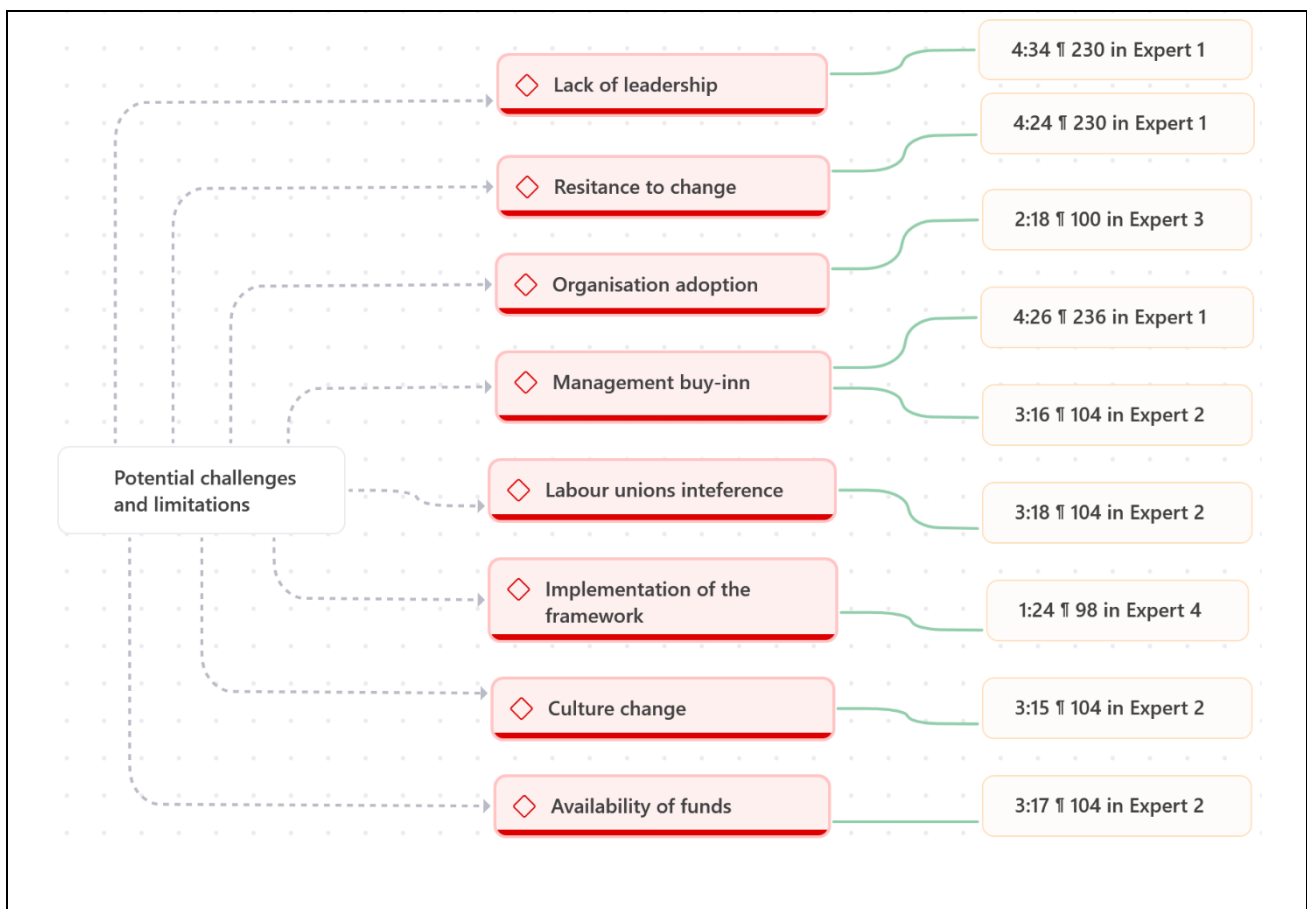


Figure 5-16: Potential Challenges and Limitations - Thematic Network Diagram

As shown in **Figure 5-16**, experts provided different views on potential challenges. Expert 1 mentioned resistance to change as a key challenge. His input suggested that employees may hesitate to adopt new practices and policies, and that, without leadership support, implementing the ECISP Framework may be challenging.

Expert 2 mentioned labour union interference as a potential limitation or challenge in implementing the ECISP Framework. He stated that “Government departments face a number of dependencies that could affect the successful implementation of the framework. For instance,

consequence management often involves labour unions; therefore, organisations must engage with them to gain their support.” He further mentioned the need for organisational culture change and for funds to be available. He also stated that “Implementing certain initiatives of the framework requires financial resources, which can be challenging given the current financial constraints of the South African government.”

Furthermore, both Expert 1 and Expert 2 mentioned management buy-in as another potential challenge. This implies that without strong commitment and leadership support, the implementation and sustainability of the framework may be compromised. Expert 3 mentioned organisational adoption of the framework as another challenge that could limit its implementation. This suggests that the successful implementation of the ECISP Framework depends on the organisation’s willingness and capacity to fully adopt it.

Expert 4 mentioned that implementing the framework itself is a potential challenge. He stated, *“I think the challenges might be beyond your control because the framework implementation will be done and managed by the various government departments. If organisations decide not to follow it, then it will not be effective. As I said, from the framework itself, I don't see any issues, but implementation might be the challenge. If it is not implemented, then the current issues that you want to address in government departments will not be addressed.”*

This feedback suggests that although the refined ECISP Framework was validated by experts as a tool that can help government departments enhance end-user compliance with ISP, its success depends on various organisational factors, such as resistance from labour unions, cultural change, financial constraints, management buy-in, and organisational willingness and capacity to adopt the framework.

5.3.2.2 Validated ECISP Framework

The validation of the refined ECISP Framework informed its update. The experts recommended additional components and factors. These recommendations were reviewed and incorporated into the framework to enhance its accuracy, comprehensiveness, effectiveness, applicability, and relevance within government departments.

These improvements included the addition of an information security culture component, including factors such as leadership commitment and tone at the top, the integration of

information security practices into daily activities, employee accountability, recognition awards, and culture alignment. Other proposed factors were analysed, aligned and captured under suitable components within the framework. These include factors such as integrating security awareness into performance agreements, the IS Steering Committee, the use of AI-based monitoring and awareness tools, KPI for ISP awareness, and strengthening the monitoring mechanism.

Figure 5-17 presents the validated ECISP Framework incorporating the proposed improvements from information security experts. The proposed factors and components, derived from the thematic analysis of the information security expert interviews, are represented by diamonds (❖) with bullet points next to them, whereas the initial and refined components are represented with standard bullet points and asterisks, respectively.

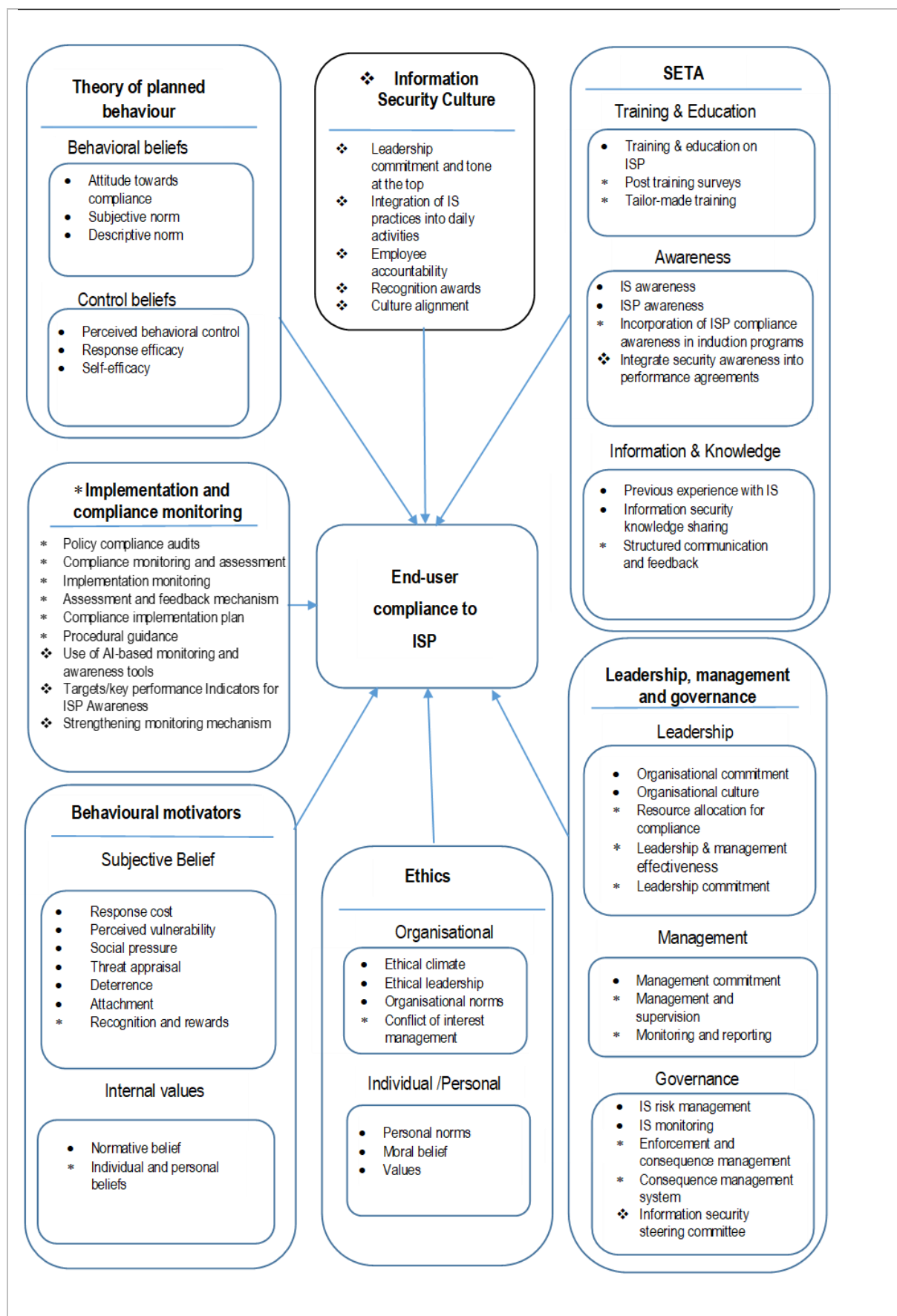


Figure 5-17: Validated Framework/ ECISP Framework

5.3.2.3 Explanation of Factors

This section explains the factors and how they can help enhance end-user compliance with ISP, in line with expert recommendations. The factors are outlined in **Table 5-2** below. Factors 1-25 were derived from the literature, and factors 29-58 were derived from the interviewees' input during the interview phases and are indicated by (*).

Table 5-2: Explanation of Factors

No	Factor	Explanation
Factors identified through the literature		
1.	Attitude towards compliance	End-users' attitude towards compliance influences their intention to comply (Kolkowska et al., 2017). Organisations should promote a positive attitude towards compliance, enabling users to view it as a positive action and increasing the likelihood of adherence.
2.	Subjective norm	Refers to the social pressures perceived by the end-user that influence certain behaviour (Ajzen, 1991). Subjective norm has a positive influence on ISP compliance (Ali et al., 2021). If employees believe that their peers, supervisors, or departments expect compliance, they are more likely to adhere. Organisations can use leadership modelling and peer influence to strengthen these perceptions.
3.	Descriptive norm	Descriptive norms refer to an individual's perception of how others behave (Cialdini et al., 1991). Descriptive norms have been recognised as a key factor influencing compliance with information security policies (Ali et al., 2021). When users see that most colleagues follow security policies, they are more likely to do the same. Organisations can create a positive perception through highlighting examples of adherence to ISP, thereby shaping employees' perception of what constitutes typical behaviour.
4.	Perceived behavioural control	An individual's perception of their ability to perform a behaviour effectively (Ajzen, 1991). Perceived behavioural control, along with subjective norms, plays a significant role in shaping an individual's behavioural intent (Ali et al., 2021). Organisations can enhance perceived behavioural control by providing resources, training and support to facilitate ISP compliance, as well as ensuring that security measures are user-friendly.
5.	Self-efficacy	Self-efficacy reflects individuals' belief in their own capability to execute specific tasks or behaviours (Bandura, 1997). Self-efficacy positively impacts compliance with the information security policies, as individuals who believe in their ability to perform secure behaviours are more likely to adhere to the policy requirements (Ali et al., 2021). Organisations can enhance self-efficacy by educating users about the potential consequences of security breaches.
6.	Training & education on the ISP	Regular training equips users with the knowledge and skills needed to follow policies (Nasir, 2023).
7.	IS awareness	Ongoing information security awareness campaigns help reinforce desired behaviours over time (Alotaibi & Alfehaid, 2018).
8.	ISP awareness	Specific awareness efforts focused on policy content, enhancing responsibility for security behaviour, thereby improving compliance (Balagopal & Mathew, 2024).

No	Factor	Explanation
9.	Previous experience with the ISP	Employees who have prior exposure to information security practices may demonstrate better compliance due to familiarity (Ali et al., 2021).
10.	Information security knowledge sharing	Encouraging knowledge exchange among the employees helps build a more informed workforce on information security issues (Bada & Nurse, 2019).
11.	Involvement of IS users in IS work	Actively involving end users in information security tasks shapes employees' attitudes toward compliance and fosters a sense of ownership, thereby increasing their commitment to complying with ISP requirements (Karim et al., 2021).
12.	IS Knowledge	When users possess solid knowledge, understanding, and skills in information security, they are better equipped to make informed decisions and consistently comply with the ISP requirements (Ali et al., 2021).
13.	Visibility of IS policies	When information security policies are visible, through posters and other visual advertisements, they remain top-of-mind for users, thereby enhancing the likelihood of consistent compliance (Alzahrani, 2021).
14.	Organisational commitment	Visible, consistent commitment from the organisation to enforce and support ISP builds trust and motivation (Valencia, 2022). When users feel that management truly values security, they are more likely to follow the policies.
15.	Organisational culture	An organisation's culture significantly affects how employees respond to information security policies. By fostering a dedicated security-focused subculture, organisations can encourage greater staff compliance (Solomon & Brown, 2020).
16.	IS risk management	IS risk management is regarded as one of the IS behavioural protection mechanisms (Assefa & Tensaye, 2021). By managing risks well, organisations can reduce the likelihood of policy breaches.
17.	IS monitoring	Information security monitoring has a strong influence on how employees behave towards compliance (Ali, et al., 2021). Continuous monitoring of information security and user behaviour provides early warnings of suspicious activity. This enables timely intervention, which can prevent incidents and reinforce compliant behaviour.
18.	Ethical climate	The ethical climate of an organisation influences the ISP compliance behaviour (Yazdanmehret et al., 2024). When users perceive their environment as ethically sound, they are more likely to act in accordance with the ISP.
19.	Ethical leadership	Ethical leadership influences employees' IS behaviour (Xue et al., 2021). It fosters an environment where following the ISP is viewed as a moral responsibility.
20.	Organisational norms	Organisational norms, particularly the beliefs and priorities demonstrated by top management regarding information security, significantly shape individual employees' personal norms (Dong et al., 2021). When leadership actively supports and communicates the importance of ISP compliance, employees tend to internalise these values, and their personal sense of responsibility towards adhering to security policies increases.
21.	Personal norms	Personal norms are internalised moral obligations that guide behaviours (Schwartz, 1977). Personal norms serve as a foundation for shaping attitudes, and a positive attitude toward compliance strongly influences the intention to comply with information security policies. To effectively promote ISP compliance, organisations should foster strong personal norms among employees and ensure that supportive conditions and resources are in place to enable and encourage compliant behaviour (Wiafe et al., 2020).
22.	Moral belief	When employees view safeguarding information as a moral responsibility, they demonstrate a stronger commitment to

No	Factor	Explanation
		comply with organisational security policies (D'Arcy et al., 2009). This alignment between moral obligation and ethical standards reinforces secure behaviour, making non-compliance less likely.
23.	Values	Organisational values shape the underlying assumptions and behaviours that drive compliance, understanding and aligning espoused values with security objectives is essential for improving ISP compliance. This alignment not only reinforces desired security behaviours but also enhances the overall effectiveness of cybersecurity strategies by embedding them within the organisation's cultural fabric (Handri et al., 2024).
24.	Response cost	Response cost refers to the perceived effort or inconvenience of complying with ISP or performing a protective behaviour (Maddux & Rogers, 1983). Individuals' choices regarding specific security behaviours are significantly influenced by their perceptions of the effort or inconvenience associated with the compliance behaviour. When users perceive compliance with information security policies as overly burdensome or time-consuming, they are less likely to adopt the desired security behaviours (Ali et al., 2021). Reducing this cost, for example, by simplifying procedures or providing an automated tool, can significantly improve compliance rates.
25.	Perceived vulnerability	An individual's assessment of their risk of experiencing a negative event or outcome. It influences motivation to engage in protective behaviours (Rogers, 1975a). Perceived vulnerability positively influences compliance with information security policies (Ali et al., 2021). When users feel that they or their organisation are vulnerable to cyber threats, they are more likely to engage in positive security behaviours.
26.	Social pressure	The influence exerted by others that encourages an individual to change their attitudes, values, or behaviours to conform to group norms (Asch, 1955). Social pressure positively influences employees' behaviour (Ali et al., 2021). When there is social pressure to conform to the ISP, especially in a team setting, users are more likely to conform to avoid disapproval or being singled out.
27.	Threat appraisal	Threat appraisal involves evaluating the seriousness and likelihood of a threat (Danylak et al., 2025; Maddux & Rogers, 1983). The threat appraisal process encourages employees to evaluate the severity and likelihood of security threats, thereby increasing their motivation to adhere to information security policies (Danylak et al., 2025). Users who understand the real risks associated with non-compliance are more likely to act cautiously and adhere to the ISP. Organisations should communicate the risks associated with non-compliance.
28.	Deterrence	Deterrence is defined as the use of threats or punishment to discourage individuals from engaging in undesirable behaviours. (Johnson, 2019). Deterrence positively influences ISP compliance behaviour/intention to comply (Siponen et al., 2022). The presence of penalties or consequences for non-compliance can serve as a deterrent. When users are aware that violations are monitored and penalised, they are more likely to avoid risky behaviours.
29.	Attachment	Refers to employees' emotional bond and commitment to their organisation which shapes their attitudes, and interacts with the organisation (Greškovičová, & Lisá, 2023). Individuals who feel a strong sense of belonging and commitment are more likely to comply with an organisation's policies. Attachment can be enhanced through effective communication about the importance of ISP, employee involvement in policy reviews, and recognition and reward.

No	Factor	Explanation
30.	Normative belief	Normative belief refers to what individuals think others expect them to do (Ajzen, 1991). Normative beliefs, such as positive social pressure, along with established habits, significantly influence individuals' intentions to comply with information security policies (Aebissa et al., 2024). If users believe that their peers and superiors expect compliance, they are more likely to meet those expectations. Organisations can leverage this by promoting positive norms, role models and leadership, communication campaigns.
31.	Individual and personal beliefs	Personal beliefs have a positive influence on ISP compliance (Alassaf & Alkhalifah, 2021b). Educating users and shaping these beliefs through communication and training can lead to more secure behaviours.
Factors identified through interviews		
32.	* Policy compliance audits	Regular audits help monitor adherence to the ISP requirements and identify compliance gaps. When employees know audits are conducted and taken seriously, it fosters accountability and reinforces the importance of following policies.
33.	* Compliance monitoring and assessment	Ongoing monitoring and assessments evaluate both behavioural trends and procedural effectiveness. This ensures policies are adapted to real-world behaviour. Through monitoring, organisations can target areas needing improvement.
34.	* Compliance implementation plan	A plan detailing the actions needed to effectively comply with the ISP.
35.	* Allocation of resources	Resource constraints, such as a lack of funding, staff, or tools, can hinder policy implementation. Addressing this through effective budgeting and prioritisation ensures users have what they need to comply.
36.	* Procedural guidance	Clear step-by-step procedures for complying with security requirements reduce confusion and errors. When guidance is simple and accessible, users are more likely to follow it correctly.
37.	* Use of AI-based monitoring and awareness tools	AI tools can detect threats in real time and personalise awareness training based on user behaviour. These technologies improve efficiency and make compliance efforts more adaptive and impactful.
38.	* Targets/key performance indicators for ISP awareness	Setting measurable objectives for awareness levels encourages consistent evaluation and improvement.
39.	* Strengthening the monitoring mechanism	Enhancing how compliance is tracked ensures violations are detected early and addressed effectively. Strong monitoring deters non-compliance and encourages accountability.
40.	* Leadership commitment and tone at the top	When leadership visibly supports the ISP, it sends a strong message about its importance. This top-down commitment can shape organisational culture and motivate employees to follow suit.
41.	* Integration of IS practices into daily activities	Embedding secure behaviours into daily workflows ensures they become routine. Making ISP a natural part of work rather than an extra task promotes long-term compliance.
42.	* Employee accountability	Holding employees accountable for their actions can reinforce the importance of ISP compliance.
43.	* Recognition awards	Acknowledging individuals or teams for exemplary security behaviours can motivate others to comply.
44.	* Culture alignment	Aligning ISP initiatives with organisational values and culture ensures they are better received and more likely to be internalised. When compliance is seen as part of “how we work,” it becomes more sustainable.
45.	* Post-training surveys	Surveys after training sessions provide feedback on user understanding and satisfaction. This information helps refine training content and ensure it effectively supports compliance goals.
46.	* Tailor-made training	Customising training to suit different needs or skill levels increases its relevance. When users see that training directly

No	Factor	Explanation
		addresses their tasks and gaps, they are more likely to engage with and retain the information.
47.	* Incorporation of ISP compliance awareness in induction programmes	Introducing ISP awareness during onboarding sets expectations from the start. New employees quickly understand the importance of security and are more likely to develop compliant habits.
48.	* Integrating security awareness into performance agreements	Tying security responsibilities to performance appraisals reinforces accountability. It shows that ISP compliance is not optional, but a formal part of each employee's role.
49.	* Resource allocation for compliance	Allocating adequate resources, such as staff, time, and technology, demonstrates the organisation's commitment to ISP compliance. When users have access to necessary tools and support, they are more likely to comply effectively.
50.	* Leadership & management effectiveness	Effective leadership provides clear direction, sets expectations for compliance behaviour, and encourages teams to follow suit, thereby normalising ISP adherence.
51.	* Leadership commitment	When leadership consistently supports and prioritises ISP initiatives, it sends a clear message about their importance. This commitment helps embed compliance into the organisational culture and motivates staff to follow through.
52.	* Management commitment	Management support ensures compliance in daily operations.
53.	* Management and supervision	Direct supervision ensures that employees are adhering to ISP protocols.
54.	* Structured communication and feedback	A structured approach to communicating to ensure that information reaches every employee and includes a feedback mechanism. This would allow government departments to monitor progress and develop continuous improvement strategies based on the feedback received.
55.	* Monitoring and reporting	Ongoing monitoring and timely reporting of ISP adherence help organisations identify non-compliance and address it before it escalates.
56.	* Enforcement and consequence management	Having clear consequences for non-compliance discourages violations. Enforcement measures ensure that policies are taken seriously.
57.	* Consequence management system	A formal "consequence management system" to address non-compliance. This would clarify the consequences of noncompliance with the policy and encourage end-users to comply.
58.	* Information steering committee	A dedicated committee overseeing the ISP implementation ensures alignment with organisational goals. It provides strategic direction, resolves issues, and facilitates leadership buy-in.
59.	* Recognition and rewards	Acknowledging and rewarding compliance encourages positive reinforcement. Users are more likely to follow the ISP when their efforts are noticed and appreciated by management.
60.	* Consequence management	Clear and fair consequence management ensures accountability. It demonstrates that the ISP violations have repercussions, thereby reinforcing the importance of compliance.
61.	* Conflict of interest management	Managing conflicts of interest ensures that personal gain does not override compliance responsibilities.

5.4 SUMMARY

This chapter outlined the refinement and validation of the ECISP Framework. Feedback from interviews with government officials and information security experts was used to refine and validate the framework. The refinement and validation included adding and amending some components and factors. This resulted in the incorporation of two new components into the

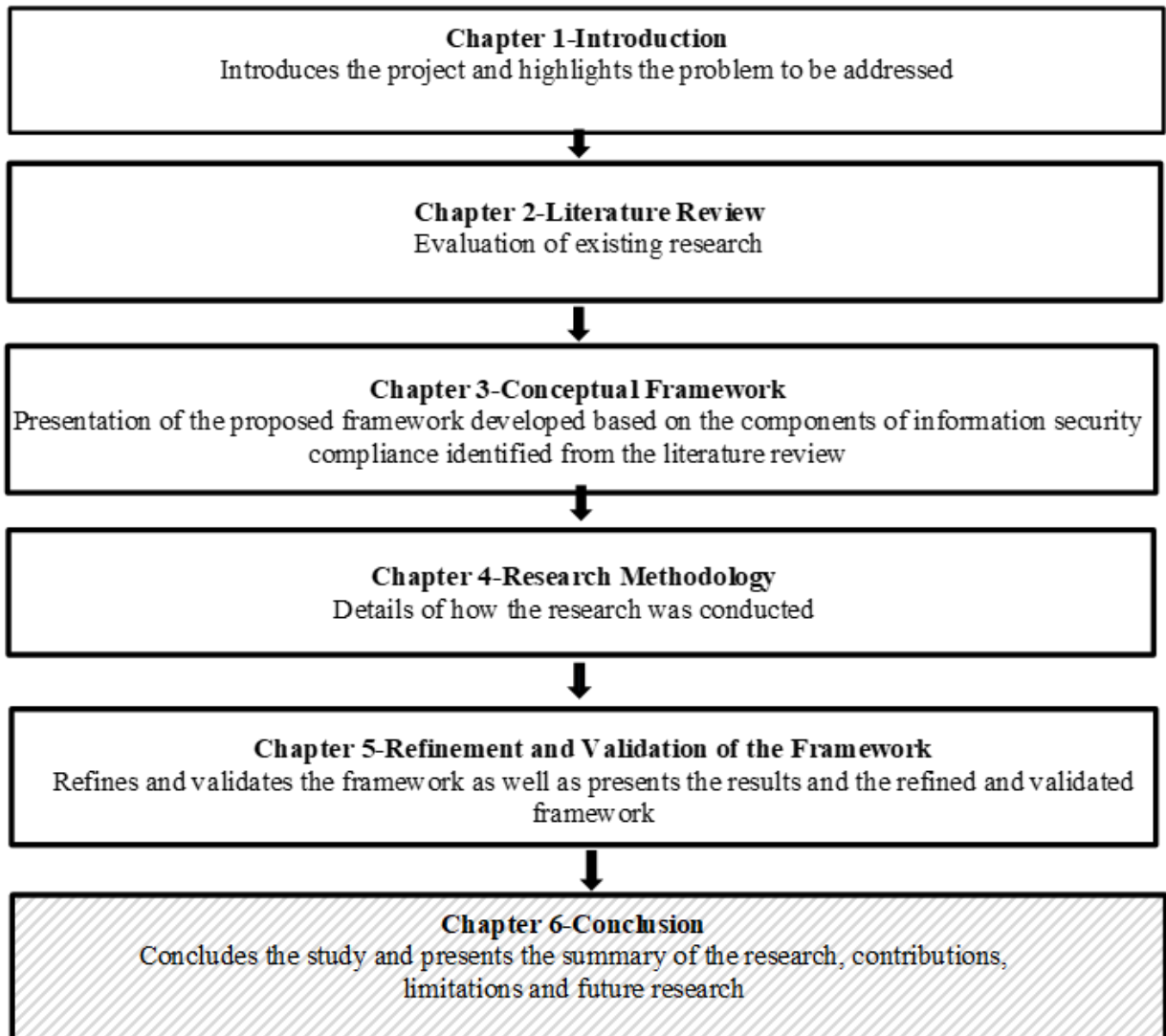
framework. The first component incorporated is “Implementation and Compliance Monitoring,” with proposed relevant factors including policy compliance audits; compliance monitoring and assessment; implementation monitoring; feedback mechanisms; compliance implementation plans; procedural guidance; AI-based monitoring and awareness tools; ISP awareness KPIs; and strengthened monitoring mechanisms.

The second component added is “Information Security Culture,” with proposed relevant factors including leadership commitment and tone at the top, integration of security practices into daily operations, employee accountability, recognition awards, and culture alignment.

In addition to these new components, several relevant factors were added to four of the initially proposed components. For SETA, these included post-training surveys, tailor-made training, incorporation of ISP compliance into induction programmes, and integration of information security awareness into performance agreements. Leadership, Management and Governance were expanded to include resource allocation for compliance, leadership and management effectiveness, leadership commitment, management and supervision, monitoring and reporting, enforcement and consequence management, compliance management system, and the formation of an IS Steering Committee. Under Ethics, conflict-of-interest management was added, while Behavioural Motivators was updated to include recognition and rewards, consequence management, and individual and personal beliefs.

The proposed additions from government officials informed the refined ECISP Framework (**Figure 5-7**), while those suggested by experts were incorporated into the validated version of the ECISP Framework (**Figure 5-17**). Through these enhancements, this chapter successfully addressed the main research question and fulfilled the study’s objective of developing a comprehensive ECISP Framework tailored for South African government departments. The next chapter presents a summary of the research study.

6. CHAPTER 6: CONCLUSION



6.1 INTRODUCTION

The previous chapter introduced the validated ECISP Framework for government departments in South Africa. This chapter presents the study's conclusion. This phase is defined as the concluding step in Yin's (2003) case study approach.

The main objective of the research was to develop an ECISP Framework for government departments in South Africa. The research study applied the Yin (2003) Case study method to develop the ECISP Framework. This chapter addresses the research questions and provides a synopsis of the research study.

6.2 OVERVIEW OF CHAPTER 6

This chapter begins with a review of the study's research problem (section 6.3). Section 6.4 reflects on the research questions. A summary of the research method and the chapters is provided in sections 6.5 and 6.6, respectively. Sections 6.7 and 6.8 present the contributions and limitations of the research study, respectively. Future research is outlined in section 6.9, 6.10 outlines the appendices attached in this research report and the conclusion is presented in section 6.11.

6.3 REVIEW OF THE RESEARCH PROBLEM

One of the key factors affecting organisations is information security. According to Alassaf & Alkhalifah, (2021) and Safa et al. (2016), information security is a challenge in organisations. This is because installing the right technology does not guarantee that information is properly secured. Human factors have been identified as key sources of information security risks in organisations (Assefa & Tensaye, 2021). Organisations have developed good information security policies, but employee compliance is a challenge (Topa & Karyda, 2015). The focus of research studies associated with ISP compliance has predominantly been on identifying the factors that affect employees' non-compliance and compliance with ISP (Shih & Liou, 2015; Safa et al., 2016; Topa & Karyda, 2015).

Most research on ISP compliance has focused on the banking and health sectors; few studies have examined ISP compliance in the government sector. Government institutions are also experiencing data breaches that result in the loss of critical information and resources, causing economic damage (Caryn, 2021; Toyana, 2021). Furthermore, online criminals are increasingly targeting some of South Africa's most crucial government departments (Caryn, 2021). Most attackers use ransomware, distributed via phishing emails or by utilising compromised user login details (Rick Crouch & Associates private investigators, 2021). These types of attacks require end-user action, such as clicking a malicious link or opening a harmful attachment, to be successful (Klevchuk, 2021). Hence, enhancing end-user compliance with ISP, leveraging key factors such as security training and awareness programmes, as well as continuous information systems monitoring, can help improve end-user behaviour and reduce data breaches in organisations (Klevchuk, 2021; Trarynny, 2025).

In addition, most studies focus on identifying factors that enhance end-user compliance without developing a framework. Studies conducted by other researchers do not provide a framework for government institutions to improve end-user information security compliance. This study proposes a validated ECISP Framework that consolidates all factors that enhance ISP compliance within the South African government.

6.4 REFLECTION ON RESEARCH QUESTIONS

The main research question of the study was:

What elements constitute a framework for end-user information security policy compliance within a government institution in South Africa?

In order to respond to the main research question, the following sub-research questions were examined:

- SRQ1: *What does existing research reveal about the current state and the factors affecting end-user compliance with the ISP?*

This sub-research question assessed the available relevant literature to identify components of the proposed framework. As shown in **APPENDIX A**, selected research studies were assessed based on their research focus. **Error! Reference source not found.** lists factors that enhance end-user compliance with ISP, identified from the available literature. The table shows 57 factors associated with behavioural motivators, 15 with Security Education, Training, and Awareness (SETA), 9 with the Theory of Planned Behaviour, 20 with leadership, management, and governance, and 9 with ethical considerations.

The table results indicate the following: Firstly, the limited number of studies focused on developing and validating ISP compliance frameworks indicates a notable gap in this research area. Secondly, the scarcity of research targeting government departments suggests that ISP compliance within this context remains underexplored. Thirdly, although some studies examine ISP compliance in public sector settings, there is a significant lack of research specifically focused on end-user compliance within South African government institutions. Fourthly, the most frequently applied theoretical models in ISP compliance research are Deterrence Theory, the Theory of Planned Behaviour, and Protection Motivation Theory. Finally, there is currently no

standardised framework available to support and enhance end-user compliance with the ISP in government departments that already have existing policies in place.

- SRQ2: *How can the existing literature help constitute a conceptual framework for end-user compliance with information security policy?*

This sub-research question assessed the development of the conceptual ECISP Framework using the identified components. The assessment result assisted in the development of the conceptual ECISP framework with components and factors that affects end-user compliance with ISP. The conceptual ECISP framework formed the basis of the initial structure and factors, components and relationships that are expected to improve end-user compliance with ISP in government departments. The outcome of this sub-research question is shown in **Error! Reference source not found.**, and the process of developing the conceptual framework included identifying the components of the ECISP Framework in **Error! Reference source not found.**. The components were established based on the factors identified from the literature review. TPB was included as one of the components because it was used by most of the assessed studies that identified factors that affects end-user compliance with ISP. TPB also relates to behavioural factors and aligns with the study's purpose. The conceptual framework was used to develop interview questions based on the factors and components identified from existing literature. The factors included in the framework were selected based on their frequency of mention in the existing literature to reflect their relevance and significance. Ethics-related factors were maintained despite being mentioned less frequently, as they are among the components that affect policy compliance in the South African government (Department of Public Service and Administration, 2013). A total of 33 factors and 5 components were subsequently used to develop the conceptual framework.

- SRQ 3: *What elements constitute a validated framework for end-user ISP compliance within a government institution in South Africa?*

This sub-research identifies the key components and factors to include in a validated ECISP Framework. The results of interviews with government officials and information security experts were used to refine and validate the conceptual ECISP Framework and the refined ECISP Framework, respectively. During this process, participants also proposed additional relevant factors (leadership commitment and tone at the top, integration of IS practices into

daily activities, employee accountability, recognition awards, culture alignment, post-training surveys, tailor-made training, incorporation of ISP compliance awareness in induction programmes, integration of security awareness into performance agreements, structured communication and feedback, resource allocation for compliance, leadership and management effectiveness, leadership commitment, management and supervision, monitoring and reporting, enforcement and consequence management, consequence management system, information security steering committee, conflict of interest management, policy compliance audits, compliance monitoring and assessment, implementation monitoring, assessment and feedback mechanism, compliance implementation plan, procedural guidance, use of AI-based monitoring and awareness tools, targets/key performance indicators for ISP awareness, strengthening the monitoring mechanism, recognition and rewards, individual and personal beliefs and components (implementation and compliance monitoring, information security culture). These additional factors and components were incorporated into the ECISP Framework to enhance its applicability and relevance to the government department's settings.

Figure 5-17 presents the outcome of the refinement and validation process: a validated ECISP Framework. This outcome answers the sub-research question by outlining the key components and factors required to enhance end-user ISP compliance in government institutions.

- Main research question: *What elements constitute a framework for end-user ISP compliance within a government institution in South Africa?*

The main research question is to identify the key elements that constitute an end user's compliance with the ISP framework in a government institution. This includes the outcomes of SRQ2 and SRQ3, where SRQ2 helped develop a conceptual ECISP framework through the use of existing literature, while SRQ3 enabled the refinement and validation of the conceptual ECISP framework through interviews with government officials and expert reviews respectively. The outcome was the final ECISP framework which presents the integrated elements that can help government departments in enhancing end-user compliance with ISP, thereby answering the main research question. The final validated ECISP Framework is presented in **Figure 5-17**.

6.5 SUMMARY OF THE RESEARCH DESIGN

This study was conducted using a qualitative research approach, applying Yin's (2003) case study method. The research design followed Yin's three key phases: Define and Design; Prepare, Collect and Analyse; and Conclude.

Phase 1: Define and Design

The research questions were defined, and the case study approach was selected. This phase involved reviewing the relevant literature to identify the factors and components of the proposed ECISP Framework. This phase addressed SRQ1: *What does existing research reveal about the current state and the factors affecting end-user compliance with ISP?*

Phase 2: Prepare, Collect and Analyse

The following steps were followed to develop, refine, and validate the conceptual ECISP Framework:

- **Step 1: Conceptual Framework Development**

In Chapter 3, the conceptual ECISP Framework was developed using factors and components identified through a literature review. This step answered SRQ2: *How can the existing literature help constitute a framework for end-user compliance with ISP?*

- **Step 2: Refine the Framework**

In Chapter 5, the conceptual ECISP Framework was refined based on feedback from interviews with government officials.

- **Step 3: Validate the Framework**

In Chapter 5, the refined ECISP Framework was validated using feedback received from information security experts. The results were used to present the final validated ECISP, which answers SRQ3: *What elements constitute a validated framework for end-user ISP compliance within a government institution in South Africa?*

The results of Phase 2 are depicted in Chapters 3, 5, and 6. These chapters present the development, refinement and validation process of the ECISP Framework.

Phase 3: Conclusion and Recommendation

This final phase outlines the study's findings and presents recommendations. Chapter 6 answers the Main RQ: *What elements constitute a framework for end-user ISP compliance within a government institution?*

By following Yin's (2003) case study methodology, the study incrementally developed, refined, and validated the ECISP Framework for government institutions.

6.6 SUMMARY OF RESEARCH CHAPTERS

This section provides the summary of the research chapters from Chapter 1 to Chapter 6.

Chapter 1 – Introduction

Chapter 1 introduced the research study, provided the background and the study rationale, outlined the research problem, the research questions and objectives, ethical considerations, and gave a brief overview of the research methodology.

Chapter 2 – Literature Review

Chapter 2 presented the systematic literature review that was used to identify key factors and components relevant to the development of the ECISP Framework. In this chapter, existing research was used to identify and present a list of factors that can enhance end-user compliance with ISP.

Chapter 3 – Conceptual Framework

Based on the results of the literature review, Chapter 3 analyses the identified factors in order of relevance and outlines the categories used to establish the components. Based on this analysis, a conceptual framework was developed to serve as the basis for the ECISP Framework.

Chapter 4 – Research Methodology

Chapter 4 outlined the research approach used to develop the ECISP Framework. Yin's case study method was applied with its respective phases. This chapter also described the data collection process, which consisted of semi-structured interviews with government officials and information security experts. Ethical clearance for the study was also outlined in this chapter.

Chapter 5 – Refinement and Validation of the Proposed ECISP Framework

In Chapter 5, the conceptual framework was refined and validated through two consecutive phases. First, feedback from government officials was used to refine the ECISP Framework; second, feedback from information security experts was used to validate the refined ECISP Framework. As a result, the final validated ECISP framework was produced.

Chapter 6 – Final Discussion and Conclusion

Chapter 6 provides an overview of the research study, outlining the research problem, the main and sub-research questions, and the objectives, and summarising the research design and the chapters. It also outlines the contributions of the validated ECISP Framework, presents the limitations, and provides recommendations for implementation, as well as suggesting areas for future research.

6.7 RESEARCH CONTRIBUTIONS

The study aimed at developing an ECISP Framework for government departments in South Africa. Yin's (2003) case study research methodology, including its phases, was employed to develop, refine, and validate the ECISP framework.

The ECISP Framework enhances end-user compliance with the ISP in government departments, thereby assisting the government in reducing the risk of data breaches caused by end users. The research contributes by developing and presenting a validated ECISP Framework aligned with the information security needs of government departments in South Africa. Implementing the validated ECISP Framework will assist government departments in preventing financial and reputational losses resulting from cybercrime-related information losses (CISCO, 2021).

The key knowledge contribution of this study is the development of a consolidated ECISP Framework to enhance end-user ISP compliance within South African government institutions. Although several studies have examined information security across different sectors, there has been limited focus on developing a consolidated, validated framework to enhance end-user ISP compliance in government settings. The 33 initial factors, together with the additional factors, provide a holistic consolidation of behaviour-related factors for ISP compliance. Moreover, an ECISP Framework aligned with and relevant to the South African government context has not been developed. Consequently, the key contribution of this study is the development of the

validated ECISP Framework to help South African government institutions enhance end-user compliance with ISP.

6.8 LIMITATIONS

The study is limited to the South African government context. Inputs from the refinement and validation processes were gathered through interviews with South African government officials and information security experts. Therefore, the findings and framework components align with this context. The framework does not reflect perspectives from other countries or industries; therefore, it may not be fully applicable to them without contextual adaptation.

Secondly, the framework was not tested in a real-world setting. Although government officials and expert interviews were used to refine and validate the ECISP Framework, experimental testing within government departments is necessary to assess its effectiveness, usability, and adaptability in real-world settings.

Furthermore, the study used qualitative interviews as the primary data collection method, with a sample of 18 participants (government officials and experts), out of these participants, the government officials were from one province. Although the sample size is sufficient for a qualitative study, it may not fully represent the diverse experiences and views across all government departments in South Africa.

Lastly, information security threats are evolving rapidly, as reflected in changes to compliance requirements. The framework may therefore require regular updates to remain current.

6.9 FUTURE RESEARCH

Future research can focus on conducting fieldwork to apply the ECISP Framework and verify its effectiveness in real-world settings. Government departments can use the framework to verify the completeness of their information security programs through a self-assessment to check if they address all the factors. Further research can also be conducted to customise and validate the ECISP Framework for other industries to enable wider application.

The ECISP framework will serve as a guideline for government departments on enhancing end-user compliance with ISP by providing the factors that affect end-user compliance to ISP. Further research can be conducted to develop detailed implementation guidelines that include procedures that will assist government departments in applying these factors when implementing the ECISP Framework.

6.10 CONCLUSION

This research aimed to develop an ECISP Framework that can be implemented by South African government departments. The ECISP Framework was developed using components from the systematic literature review (Chapter 2). Interviews were conducted with government officials and expert reviewers in information security and information technology. The factors and components identified through the literature review were used to develop the conceptual ECISP Framework (Chapter 3). Feedback from government officials was used to refine the ECISP Framework, and feedback from experts was used to validate it, resulting in the ECISP Framework (Chapter 5). In this chapter, the research problem and research questions were reviewed; a synopsis of the research design was provided; research limitations were outlined; and future research directions were outlined. The ECISP Framework was developed to help government institutions improve end-user compliance with information security policies and mitigate internal security risks.

7. REFERENCES

- Abdelwahed, A. S., Mahmoud, A. Y., & Bdair, R. A. (2017). . Information Security Policies and their Relationship with the Effectiveness of the Management Information Systems of Major Palestinian Universities in the Gaza Strip. *International Journal of Information Science and Management*, 15(1), 1–26. <https://ijism.ricest.ac.ir/index.php/ijism/article/view/1179>
- Aebissa, B., Dhillon, G., & Meshesha, M. (2024). Information security policy compliance: a replication study in Ethiopia. *Information and Computer Security*, 33(3), 408–426. <https://doi.org/10.1108/ICS-03-2024-0066>
- Ahmed, A. A. A., & Abas, H. (2024). Factors Influencing Information Security Policy Compliance Behavior in High Education Institutions: Systematic Literature Review. *Advances in Social Sciences Research Journal*, 11(7), 260–273. <https://doi.org/10.14738/assrj.117.17308>
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Alassaf, M., & Alkhalifah, A. (2021). Exploring the Influence of Direct and Indirect Factors on Information Security Policy Compliance: A Systematic Literature Review. *IEEE Access*, 9, 162687–162705. <https://doi.org/10.1109/ACCESS.2021.3132574>
- Alenezi, A., Atlam, H. F., & Wills, G. B. (2019). Experts reviews of a cloud forensic readiness framework for organizations. *Journal of Cloud Computing*, 8(1). <https://doi.org/10.1186/s13677-019-0133-z>
- Alfawaz, S., Nelson, K., & Mohannak, K. (2010, January). Information security culture: a behaviour compliance conceptual framework. *8th Australasian Information Security Conference (AISC 2010)*, 105, 47–55). University of Southern Queensland. <https://dl.acm.org/doi/10.5555/1862266.1862275>
- Alharahsheh, H. H., & Pius, A. (2020). A review of key paradigms: Positivism VS interpretivism. *Global academic journal of humanities and social sciences*, 2(3), 39-43. <https://garjc.com/doi/10.36348/gajhss.2020.v02i03.001>
- Ali, R. F., & Dominic, P. D. D. (2024). Investigation of information security policy violations among oil and gas employees: A security-related stress and avoidance coping perspective. *Journal of Information Science*, 50(1), 254–272. <https://doi.org/10.1177/01655515221087680>
- Ali, R. F., Dominic, P. D. D., & Ali, K. (2020). Organizational governance, social bonds and information security policy compliance: a perspective towards oil and gas employees. *Sustainability (Switzerland)*, 12(20), 1–27. <https://doi.org/10.3390/su12208576>
- Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: a systematic literature review for

- identifying the transformation process from noncompliance to compliance. *Applied Sciences (Switzerland)*, 11(8). <https://doi.org/10.3390/app11083383>
- Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., & Aleassa, H. (2013). Information security policy compliance: An empirical study of ethical ideology. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 3018–3027. <https://doi.org/10.1109/HICSS.2013.272>
- Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Security policy compliance: User acceptance perspective. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 3317–3326. <https://doi.org/10.1109/HICSS.2012.516>
- Alotaibi, M., & Alfehaid, W. (2018). Information Security Awareness: A Review of Methods. Challenges and Solutions, *Proceedings of the ICITST-WorldCIS-WCST-WCICSS 2018 Conference*, 119–127. <https://doi.org/10.2053/ICITST.WorldCIS.WCST.WCICSS.2018.0016>
- Alotaibi, M., Furnell, S., & Clarke, N. (2017). Information security policies: A review of challenges and influencing factors. *11th International Conference for Internet Technology and Secured Transactions, ICITST 2016*, 352–358. <https://doi.org/10.1109/ICITST.2016.7856729>
- Alraja, M. N., Butt, U. J., & Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. *Computers and Security*, 129, 103208. <https://doi.org/10.1016/j.cose.2023.103208>
- Alzahrani, L. (2021). Factors Impacting Users' Compliance with Information Security Policies: An Empirical Study. *International Journal of Advanced Computer Science and Applications*, 12(10), 437–447. <https://doi.org/10.14569/IJACSA.2021.0121049>
- Amankwa, E., Looock, M., & Kritzinger, E. (2022). The determinants of an information security policy compliance culture in organisations: the combined effects of organisational and behavioural factors. *Information and Computer Security*, 30(4), 583–614. <https://doi.org/10.1108/ICS-10-2021-0169>
- Archer, E., Janse van Vuuren, H. H., & Van der Walt, H. D. (2017). *Introduction to Atlas.ti: Basic operations, tips and tricks for coding* (6th Edition) Research Rescue. <https://uir.unisa.ac.za/handle/10500/23000>
- Arcy, J. D., & Teh, P. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management*, 56(7), 103151. <https://doi.org/10.1016/j.im.2019.02.006>
- Asch, S. E. (1955). Opinions and Social Pressure. *Scientific American*. *Scientific American*, 193(5), 31–35. <https://doi.org/10.1038/scientificamerican1155-31>

- Askey, H., & O'Malley, L. (2009). Scoping studies: towards a methodological framework. *International Journal of Social Research Methodology*, 8(1), 19–32.
<https://doi.org/10.1017/S0922156508005621>
- Assefa, T., & Tensaye, A. (2021). Factors influencing information security compliance: an institutional perspective. *SINET: Ethiopian Journal of Science*, 44(1), 108–118.
<https://doi.org/10.4314/sinet.v44i1.10>
- Au, N., Ngai, E. W. T., & Cheng, T. C. E. (2002). A critical review of end-user information system satisfaction research and a new research framework. *Omega*, 30(6), 451–478.
[https://doi.org/10.1016/S0305-0483\(02\)00054-3](https://doi.org/10.1016/S0305-0483(02)00054-3)
- Aurigemma, S., & Panko, R. (2012). A composite framework for behavioral compliance with information security policies. *Proceedings of the 45th Annual Hawaii International Conference on System Sciences*, 3248–3257. <https://doi.org/10.1109/HICSS.2012.49>
- Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small and medium-sized enterprises (SMEs). *Information & Computer Security*, 27(3), 393–410. <https://doi.org/10.1108/ICS-07-2018-0080>
- Balagopal, N., & Mathew, S. K. (2024). Exploring the factors influencing information security policy compliance and violations: A systematic literature review. *Computers & Security*, 147. <https://doi.org/10.1016/j.cose.2024.104062>
- Balozian, P., & Leidner, D. (2017). Review of IS Security Policy Compliance. *ACM SIGMIS Database: The Database for Advances in Information Systems*, 48(3), 11–43.
<https://doi.org/10.1145/3130515.3130518>
- Bandura, A. (1997). *Self-Efficacy: The Exercise of Control*, New York. W.H Freeman.
- Bauer, S., & Bernroider, E. W. N. (2017). From Information Security Awareness to Reasoned Compliant Action. *ACM SIGMIS Database: The Database for Advances in Information Systems*, 48(3), 44–68. <https://doi.org/10.1145/3130515.3130519>
- Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers and Security*, 68, 145–159.
<https://doi.org/10.1016/j.cose.2017.04.009>
- Beautement, A., Sasse, M. A., & Wonham, M. (2008). *The Compliance Budget: Managing Security Behaviour in Organisations*. 47–58. <https://doi.org/10.1145/1595676.1595684>
- Beris, O., Beautement, A., & Sasse, M. A. (2015). Employee Rule Breakers, Excuse Makers and Security Champions: Mapping the Risk Perceptions and Emotions That Drive Security Behaviors. *Proceedings of the 2015 New Security Paradigms Workshop*, 73–84.
<https://doi.org/10.1145/2841113.2841119>

- Bohnsack, R., Pinkse, J., & Kolk, A. (2014). Business models for sustainable technologies: Exploring business model evolution in the case of electric vehicles. *Research policy*, 43(2), 284–300. <https://doi.org/10.1016/j.respol.2013.10.014>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Bryman, A. (2004). *Social research strategies. Social Research Methods* (Second Edition). Oxford University Press.
https://books.google.co.za/books/about/Social_Research_Methods.html?id=GYrUQgAACAAJ&redir_esc=y
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Effects of individual and organization based beliefs and the moderating role of work experience on insiders' good security behaviors. *Proceedings - 12th IEEE International Conference on Computational Science and Engineering, CSE 2009*, 3, 476–481. <https://doi.org/10.1109/CSE.2009.484>
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, 34(3), 523–548. <https://doi.org/10.2307/25750690>
- Caley, M. J., O'Leary, R. A., Fisher, R., Low-Choy, S., Johnson, S., & Mengersen, K. (2014). What is an expert? A systems perspective on expertise. *Ecology and evolution*, 4(3), 231–242. <https://doi.org/10.1002/ece3.926>
- Cannoy, S. D., & Salam, A. F. (2010). A framework for health care information assurance policy and compliance. *Communications of the ACM*, 53(3), 126.
<https://doi.org/10.1145/1666420.1666453>
- Caryn, D. (2021, November 6). Cyberattacks: South Africa, you've been hacked. Daily Maverick. <https://www.dailymaverick.co.za/article/2021-11-06-cyberattacks-south-africa-youve-been-hacked>
- Chen, H., & Li, W. (2019). Understanding commitment and apathy in is security extra-role behavior from a person-organization fit perspective. *Behaviour & Information Technology*, 38(5), 454–468. <https://doi.org/10.1080/0144929X.2018.1539520>
- Chen, X., Chen, L., & Wu, D. (2018). Factors that influence employees' security policy compliance: an Awareness-Motivation-Capability (AMC) perspective. *Journal of Computer Information Systems*, 58(4), 312–324. <https://doi.org/10.1080/08874417.2016.1258679>
- Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers and Security*, 39(PART B), 447–459. <https://doi.org/10.1016/j.cose.2013.09.009>

- Choi, M., & Song, J. (2018). Social control through deterrence on the compliance with information security policy. *Soft Computing*, 22(20), 6765–6772. <https://doi.org/10.1007/s00500-018-3354-z>
- Choi, Y. (2017). Human Resource Management and Security Policy Compliance. *International Journal of Human Capital and Information Technology Professionals*, 8(3), 68–81. <https://doi.org/10.4018/ijhcitp.2017070105>
- Choo, K. K. R., Heravi, A., Mani, D., & Mubarak, S. (2015). Employees' intended information security behaviour in real estate organisations: A Protection Motivation perspective. In *Proceedings of the 21st Americas Conference on Information Systems (AMCIS 2015)* 29, 1–11. Association for Information Systems. <https://aisel.aisnet.org/amcis2015/ISSecurity/GeneralPresentations/29>
- Cialdini, R. B., Kallgren, C. A., & Reno, R. R. (1991). A Focus Theory of Normative Conduct: A Theoretical Refinement and Reevaluation of the Role of Norms in Human Behavior. *Advances in Experimental Social Psychology*, 24(C), 201–234. [https://doi.org/10.1016/S0065-2601\(08\)60330-5](https://doi.org/10.1016/S0065-2601(08)60330-5)
- CISCO. (2021). Security Outcomes Report: Achieving Security Resilience (Vol. 3). <https://blogs.cisco.com/security/security-resilience-moving-beyond-the-buzzword>
- Colquhoun, H. L., Levac, D., O'Brien, K. K., Straus, S., Tricco, A. C., Perrier, L., Kastner, M., & Moher, D. (2014). Scoping reviews: Time for clarity in definition, methods, and reporting. *Journal of Clinical Epidemiology*, 67(12), 1291–1294. <https://doi.org/10.1016/j.jclinepi.2014.03.013>
- Corpuz, M.S. (2011). The Enterprise Information Security Policy as a Strategic Business Policy within the Corporate Strategic Plan. *Proceedings of the 15th World Multi-Conference on Systemics, Cybernetics and Informatics, International Institute of Informatics and Systemics (IIIS), Orlando, FL, USA*, 275–279. https://www.iiis.org/CDs2011/CD2011SCI/RMCI_2011/PapersPdf/RA717ZB.pdf
- Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behavior*, 28(5), 1849–1858. <https://doi.org/10.1016/j.chb.2012.05.003>
- Creswell, J. W. (2007). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. (Second Edition). Sage Publications.
- Creswell, J. W. (2014). *Qualitative, Quantitative and mixed methods approaches*. (Fourth Edition). Sage Publications. https://books.google.co.za/books?id=4uB76IC_pOQC&printsec=frontcover#v=onepage&q&f=false

- Creswell, J. W. & Poth, C. N. (2016). *Qualitative Inquiry & Research Design: Choosing Among 5 Approaches*. (Fourth Edition). Sage Publications.
[https://books.google.co.za/books?hl=en&lr=&id=DLbBDQAAQBAJ&oi=fnd&pg=PP1&dq=Creswell,+J.+W.+%26+Poth,+C.+N.+\(2016\).+Qualitative+Inquiry+and+Research+Design:+Choosing+Among+5+Approaches.+\(Fourth+Edition\).+Sage+Publications.&ots=-iv38eLVVy&sig=cBKalCbf8qzdOVpsJr5WrU0c5zI#v=onepage&q&f=false](https://books.google.co.za/books?hl=en&lr=&id=DLbBDQAAQBAJ&oi=fnd&pg=PP1&dq=Creswell,+J.+W.+%26+Poth,+C.+N.+(2016).+Qualitative+Inquiry+and+Research+Design:+Choosing+Among+5+Approaches.+(Fourth+Edition).+Sage+Publications.&ots=-iv38eLVVy&sig=cBKalCbf8qzdOVpsJr5WrU0c5zI#v=onepage&q&f=false)
- Cyber Security Insiders:2024 Insider Threat Report. (2024). In *Cyber Security Insiders*.
<https://doi.org/10.5040/9798216189558.0011>
- Da Veiga, A. (2015). The Influence of Information Security Policies on Information Security Culture: Illustrated through a Case Study. In S. Furnell & N. Clarke (Eds.), *Proceedings of the Ninth International Symposium on Human Aspects of Information Security and Assurance (HAISA 2015)*, 162–176. Centre for Security, Communications and Network Research, University of Plymouth. <https://www.cscan.org/openaccess/?page=proceedings>
- Danylak, P., Lins, S., & Sunyaev, A. (2025). The Role of Employees' Threat Appraisal in Security Certification Compliance: Insights from a Protection Motivation Approach. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 4502–4511. IEEE Computer Society. <https://doi.org/10.24251/HICSS.2025.541>
- D'Arcy, J. D., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, 20(1), 79–98. <https://doi.org/10.1287/isre.1070.0160>
- Delso-Vicente, A.-T., Diaz-Marcos, L., Aguado-Tevar, O., & de Blanes-Sebastián, M. G. (2025). Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity. *Future Business Journal*, 11(1), 28. <https://doi.org/10.1186/s43093-025-00452-7>
- Demissew, S., Carabias, J., Di, S., Joly, C., Lonsdale, M., Ash, N., Larigauderie, A., Adhikari, J. R., Arico, S., Bartuska, A., Baste, I. A., Bilgin, A., Brondizio, E., Chan, K. M. A., Figueroa, V. E., Duraiappah, A., Fischer, M., Hill, R., Koetz, T., Thomas, S. (2015). The IPBES Conceptual Framework — Connecting Nature and People. *Current Opinion in Environmental Sustainability*, 14, 1–16. <https://doi.org/10.1016/j.cosust.2014.11.002>
- Department of Public Service and Administration. (2013). Public sector integrity management framework. [https://www.dpsa.gov.za/dpsa2g/documents/misc/Integrity Management Framework.pdf](https://www.dpsa.gov.za/dpsa2g/documents/misc/Integrity+Management+Framework.pdf)
- Dong, K., Ali, R. F., Dominic, P. D. D., & Ali, S. E. A. (2021). The effect of organizational information security climate on information security policy compliance: the mediating effect

- of social bonding towards healthcare nurses. *Sustainability (Switzerland)*, 13(5), 1–25.
<https://doi.org/10.3390/su13052800>
- Ericsson, K., & Smith, J. (Eds.). (1991). *Towards a general theory of expertise: Prospects and limits*. Cambridge University Press. <https://www.cambridge.org/9780521406123>
- Faizi, S. M., & Rahman, S. S. M. (2020). Effect of Fear on Behavioral Intention to Comply. *ACM International Conference Proceeding Series*, 65–70.
<https://doi.org/10.1145/3404663.3404685>
- Foth, M. (2017). Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence Factors influencing the intention to comply with data protection regulations in hospitals: based on gender. *The European Journal of Information Systems*, 25(2), 91–109. <https://doi.org/10.1057/ejis.2015.9>
- Gcaza, N. (2017). A national Strategy towards Cultivating a Cybersecurity Culture in South Africa [Thesis]. Nelson Mandela Metropolitan University. [https://seals-nmu.primo.exlibrisgroup.com/nde/search?vid=27SEALS_NMU:NMU&tab=Everything&search_scope=MyInst_and_CI&query=Gcaza,%20N.%20\(2017\).%20A%20national%20Strategy%20towards%20Cultivating%20a%20Cybersecurity%20Culture%20in%20South%20Africa%20%5BThesis%5D.%20Nelson%20Mandela%20Metropolitan%20University.&offset=0&lang=en](https://seals-nmu.primo.exlibrisgroup.com/nde/search?vid=27SEALS_NMU:NMU&tab=Everything&search_scope=MyInst_and_CI&query=Gcaza,%20N.%20(2017).%20A%20national%20Strategy%20towards%20Cultivating%20a%20Cybersecurity%20Culture%20in%20South%20Africa%20%5BThesis%5D.%20Nelson%20Mandela%20Metropolitan%20University.&offset=0&lang=en)
- Greškovičová, K., & Lisá, E. (2023). *Beyond the global attachment model: Domain- and relationship-specific attachment models at work and their functions*. *Frontiers in Psychology*, 14, 1158992. <https://doi.org/10.3389/fpsyg.2023.1158992>
- Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. *Field Methods*, 18(1), 59–82.
<https://doi.org/10.1177/1525822X05279903>
- Gustafsson, J., & Gustafsson, J. (2017). *Single case studies vs. multiple case studies: A comparative study*. [Thesis]. Halmstad University. <https://www.diva-portal.org/smash/get/diva2:1064378/FULLTEXT01.pdf>
- Hamid, S., & Huda, M. N. (2025). Mapping the landscape of government data breaches: A bibliometric analysis of literature from 2006 to 2023. *Social Sciences and Humanities Open*, 11. <https://doi.org/10.1016/j.ssaho.2024.101234>
- Handri, E. Y., Sensuse, D. I., & Lusa, S. (2024). Examining Cybersecurity Culture: Trends and Success Factors. *Journal of Internet Services and Information Security*, 14(3), 330–352.
<https://doi.org/10.58346/jisis.2024.i3.020>

- Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). *Journal of Strategic Information Systems Value conflicts for information security management*. 20, 373–384.
<https://doi.org/10.1016/j.jsis.2011.06.001>
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125. <https://doi.org/10.1057/ejis.2009.6>
- Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems. *MIS Quarterly*, 28(1), 75–105.
- Hina, S., Durai, D., Panneer, D., & Benjamin, P. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers and Security*, 87.
<https://doi.org/10.1016/j.cose.2019.101594>
- Hossain, M. A., Raza, Md. A., & Rahman, J. Y. (2025). Human factors and employee resistance to adopting new cybersecurity protocols and technologies. *Computers and Security*, 87.
<https://doi.org/10.2139/ssrn.5207157>
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, 31(1), 83–95. <https://doi.org/10.1016/j.cose.2011.10.007>
- Ifinedo, P. (2017). Roles of Organizational Climate, Social Bonds, and Perceptions of Security Threats on IS Security Policy Compliance Intentions. *Information Resources Management Journal*, 31(1), 53–82. <https://doi.org/10.4018/irmj.2018010103>
- Jabareen, Y. (2009). Building a Conceptual Framework: Philosophy, Definitions, and Procedure. *International Journal of Qualitative Methods*, 8(4), 49–62.
https://doi.org/10.1177/160940690900800406?urlappend=%3Futm_source%3Dresearchgate.net%26utm_medium%3Darticle
- Jiang, R., & Zhang, J. (2023). The impact of work pressure and work completion justification on intentional non-malicious information security policy violation intention. *Computers and Security*, 130. <https://doi.org/10.1016/j.cose.2023.103253>
- Johnson, B. (2019). Do criminal laws deter crime?: Deterrence theory in criminal justice policy: A primer. Washington DC: MN House Research.
<https://www.house.mn.gov/hrd/pubs/deterrence.pdf>
- Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. *MIS Quarterly*, 39(1), 113–134. <https://doi.org/10.25300/misq/2015/39.1.06>

- Julisch, K. (2008). Security Compliance: The Next Frontier in Security Research. *Proceedings of the 2008 New Security Paradigms Workshop*, 71–74.
<https://doi.org/10.1145/1595676.1595687>
- Kabanda, S., & Mogoane, S. N. (2021, December). A conceptual framework for exploring the factors influencing information security policy compliance in emerging economies. *International Conference on e-Infrastructure and e-Services for Developing Countries*, 203–218. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-06374-9_13
- Kakar, Z. U. H., Rasheed, R., Rashid, A., & Akhter, S. (2023). Criteria for assessing and ensuring the trustworthiness in qualitative research. <https://doi.org/10.56249/ijbr.03.01.44>
- Karim, N. A., Kaur, J., & Khalib, M. N. (2021). Benefit vs Cost: Examining Factors of Intention to Comply Information Security Policy. *IEEE International Conference on Computing (ICOCO)*, 291–296. <https://doi.org/10.1109/ICOCO53166.2021.9673542>
- Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2022). The effect of perceived organizational culture on employees' information security compliance. *Computer Security*, 30(3), 382–401. <https://doi.org/10.1108/ICS-06-2021-0073>
- Kennedy, K. M. (2019). Promoting the qualitative research approach in the discipline of forensic and legal medicine: Why more qualitative work should be promoted and how that can be achieved. *Journal of Forensic and Legal Medicine*, 62(June 2018), 72–76.
<https://doi.org/10.1016/j.jflm.2019.01.009>
- Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees' information security awareness in private and public organisations: A systematic literature review. *Computers and Security*, 106. <https://doi.org/10.1016/j.cose.2021.102267>
- Kirlappos, I., Parkin, S., & Sasse, M. A. (2015a). “Shadow security” as a tool for the learning organization. *ACM SIGCAS Computers and Society*, 45(1), 29–37.
<https://doi.org/10.1145/2738210.2738216>
- Kirlappos, I., Parkin, S., & Sasse, M. A. (2015b). “Shadow security” as a tool for the learning organization. *ACM SIGCAS Computers and Society*, 45(1), 29–37.
<https://doi.org/10.1145/2738210.2738216>
- Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University*, 33, 1–26. <https://doi.org/10.1.1.122.3308>
- Klevchuk, O. (2021). *How hackers use phishing in ransomware attacks*.
<https://blog.barracuda.com/2021/07/01/how-hackers-use-phishing-in-ransomware-attacks/>
- Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method.

Journal of Strategic Information Systems, 26(1), 39–57.

<https://doi.org/10.1016/j.jsis.2016.08.005>

- Koohang, A., Anderson, J., Nord, J. H., & Paliszkievicz, J. (2020). Building an awareness-centered information security policy compliance model. *Industrial Management and Data Systems*, 120(1), 231–247. <https://doi.org/10.1108/IMDS-07-2019-0412>
- Krocak, T. J., Baran, J., Pryjma, J., Siedlar, M., Reshedi, I., Hernandez, E., Alberti, E., Maddika, S., & Los, M. (2002). Risk Management Guide for Information Technology Systems. NIST Special Publication, 800(30). <https://doi.org/10.1517/14728222.10.2.289>
- Lee, J., & Lee, M. A. (2022). Validation and usability study of the framework for a user needs-centered mHealth app selection. *International Journal of Medical Informatics*, 167. <https://doi.org/10.1016/j.ijmedinf.2022.104877>
- Li, H., Sarathy, R., Zhang, J., & Luo, X. (2014). Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal*, 24(6), 479–502. <https://doi.org/10.1111/isj.12037>
- Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45, 13–24. <https://doi.org/10.1016/j.ijinfomgt.2018.10.017>
- Li, Y. J., & Hoffman, E. (2023). Designing an incentive mechanism for information security policy compliance: An experiment. *Journal of Economic Behavior and Organization*, 212, 138–159. <https://doi.org/10.1016/j.jebo.2023.05.033>
- Liu, C., Wang, N., & Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management*, 54(28). <https://doi.org/10.1016/j.ijinfomgt.2020.102152>
- Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, 25(5), 433–463. <https://doi.org/10.1111/isj.12043>
- Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469–479. [https://doi.org/10.1016/0022-1031\(83\)90023-9](https://doi.org/10.1016/0022-1031(83)90023-9)
- Magaldi, D., & Berler, M. (2020). Semi-structured interviews. In *Encyclopedia of Personality and Individual Differences*. Springer. https://doi.org/10.1007/978-3-319-24612-3_857

- Mandal, D. (2021). Towards an Ontology for Enterprise Level Information Security Policy Analysis. *Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP 2021)*, 492–499. <https://doi.org/10.5220/0010248004920499>
- Mauco, K. L., Scott, R. E., & Mars, M. (2020). Validation of an e-health readiness assessment framework for developing countries. *BMC Health Services Research*, 20(1), 1–10. <https://doi.org/10.1186/s12913-020-05448-3>
- Mavetera, N., Moroke, N. D., & Sebetlele, A. (2015). An empirical study of staff compliance to information security policy in a South African municipality. *Corporate Ownership and Control*, 13(1), 1375–1384. <https://doi.org/10.22495/cocv13i1c11p9>
- Milicevic, D., & Goeken, M. (2013). Social factors in policy compliance - Evidence found in literature to assist the development of policies in information security management. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 4476–4484. <https://doi.org/10.1109/HICSS.2013.488>
- Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). *Preferred Reporting Items for Systematic Reviews and Meta-Analyses: Academia and Clinic Annals of Internal Medicine* 151(4), 264–269. <https://doi.org/10.1016/j.jclinepi.2009.06.005>
- Mothupi, M. C., Knight, L., & Tabana, H. (2020). Improving the validity, relevance and feasibility of the continuum of care framework for maternal health in South Africa: A thematic analysis of experts' perspectives. *Health Research Policy and Systems*, 18(1), 1–14. <https://doi.org/10.1186/s12961-020-0537-8>
- Nasir, A., Arshah, R. A., & Ab Hamid, M. R. (2017). Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture. *Proceedings of the 2017 International Conference on Information System and Data Mining*, 56–60. <https://doi.org/10.1145/3077584.3077593>
- Nasir, A., Arshah, R. A., & Hamid, M. R. A. (2020). Information Security Culture for Guiding Employee's Security Behaviour: A Pilot Study. *6th IEEE International Conference on Information Management*, 205–209. <https://doi.org/10.1109/ICIM49319.2020.244699>
- Nasir, A., Arshah, R. A., Rashid, M., & Hamid, A. (2019). A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions. *Information Security Journal: A Global Perspective*, 28(3), 55–80. <https://doi.org/10.1080/19393555.2019.1643956>
- Ng, B. Y., Kankanhalli, A., & Xu, Y. (Calvin). (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(4), 815–825. <https://doi.org/10.1016/j.dss.2008.11.010>

- Nieles, M., Dempsey, K. L., & Pillitteri, V. Y. (2017). An introduction to information security (NIST Special Publication 800-12 Revision 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-12r1>
- Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T., & Whitty, M. (2014). Understanding insider threat: A framework for characterising attacks. 2014 IEEE Security and Privacy Workshops, 214–228. <https://doi.org/10.1109/SPW.2014.38>
- Oates, B. J. (2006). Researching Information Systems (First Edit). Sage Publications.
- Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T., & Kagaya, T. (2009). Information Security Governance Framework. *Proceedings of the First ACM Workshop on Information Security Governance*, 1–6. <https://doi.org/10.1145/1655168.1655170>
- Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security*, 88. <https://doi.org/10.1016/j.cose.2019.101608>
- Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers and Security*, 31(5), 673–680. <https://doi.org/10.1016/j.cose.2012.04.004>
- Palanisamy, R., Norman, A. A., & Kiah, M. L. M. (2020). Compliance with bring your own device security policies in organizations: A systematic literature review. *Computers and Security*, 98. <https://doi.org/10.1016/j.cose.2020.101998>
- Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). Human Factors and Information Security: Individual, Culture and Security Environment. In Command, Control, Communications and Intelligence Division (Issue DSTO-TR-2484). <https://doi.org/10.14722/ndss.2014.23268>
- Peffer, K., Tuunanen, T., Gengler, C., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (2007). The Design Science Research Process: A Model for Producing and Presenting Information Systems Research. *Journal of Management Information Systems* 24(3), 45–77. <https://doi.org/10.2753/MIS0742-1222240302>
- Ponemon Institute. (2022). 2022 Cost of Insider Threats Report Global Report. <https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats/>
- Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 757–778.
- PricewaterhouseCoopers. (2018). *The Global State of Survey 2018: Singapore highlights*. PwC <https://www.pwc.com/sg/en/publications/assets/gsis-2018.pdf>
- PricewaterhouseCoopers. (2020). *The Global State of Survey 2020*. PwC. <https://www.pwc.com/gx/en/news-room/press-releases/2020/global-digital-trust-insights-survey-2021.html>

- PricewaterhouseCoopers. (2025). Digital Trust Insights survey 2025.PwC.
<https://www.pwc.co.za/en/assets/pdf/digital-trust-insights-survey-2025.pdf>
- Quinn Patton, M., & Cochran, M. (2007). A Guide to Using Qualitative Research Methodology. *Medecins Sans Frontieres*, 1–36.
- Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers and Security*, 80, 211–223. <https://doi.org/10.1016/j.cose.2018.09.016>
- Rita, C., Richey, J. D. K., & Nelson, W. A. (2014). Developmental research: studies of instructional design and development. *Handbook of Research for Educational Communications and Technology*. Springer. https://doi.org/10.1007/978-1-4614-3185-5_12
- Rick Crouch & Associates private investigators. (2021). *Cyber-Crime and South Africa*.
<http://rickcrouch.co.za/wp/cyber-crime-and-south-africa>
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, 91(1), 93–114. <https://doi.org/10.1080/00223980.1975.9915803>
- Roberts, D. J. (2021). An Analysis of Employee Information Security Policy Compliance Behavior: A Generic Qualitative Inquiry. [Doctoral dissertation, Capella University]. Rogers.
- Ryan, G. (2018). Introduction to positivism, interpretivism and critical theory. *Nurse Researcher*, 25(4), 14–20. <https://doi.org/10.7748/nr.2018.e1466>
- Sadiq Nasir, S. N. (2023). Exploring the Effectiveness of Cybersecurity Training Programs: Factors, Best Practices, and Future Directions. *Advances in Multidisciplinary and Scientific Research Journal Publication*, 2(1), 151–160. <https://doi.org/10.22624/aims/csean-smart2023p18>
- Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, 53, 65–78. <https://doi.org/10.1016/j.cose.2015.05.012>
- Safa, N.S., Von Solms, R., & Furnell, S. (2016). Information Security Policy Compliance Model in Organizations. *Computers and Security*, 56, 70–82. <https://doi.org/10.1016/j.cose.2015.10.006>
- Saleem, M., Qadeer, F., Mahmood, F., Ariza-Montes, A., & Han, H. (2020). Ethical leadership and employee green behavior: A multilevel moderated mediation analysis. *Sustainability (Switzerland)*, 12(8), 3314. <https://doi.org/10.3390/SU12083314>
- Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students* (Fifth Edition). Pearson Education. Pearson Education.
<https://catalogue.pearsoned.co.uk/educator/product/Research-Methods-for-Business-Students/9780273716860.page>

- Saunders, M. N., Lewis, P., Thornhill, A., & Bristow, A. (2015). Understanding research philosophy and approaches to theory development. In M. N. K. Saunders, P. Lewis, & A. Thornhill (Eds.), *Research methods for business students* (7th ed., pp. 122–161). Pearson Education. <https://catalogue.pearsoned.co.uk/educator/product/Research-Methods-for-Business-Students/9781292016627.page>
- Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students* by Mark Saunders, Philip Lewis and Adrian Thornhill (Eighth Edition). Pearson Education. <https://www.pearson.com/en-gb/subject-catalog/p/research-methods-for-business-students/P200000003217>
- Savarit, E. (2020). Collecting Qualitative Data. In *Practical User Research*. https://doi.org/10.1007/978-1-4842-5596-4_7
- Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics (Switzerland)*, 9(9), 1–29. <https://doi.org/10.3390/electronics9091460>
- Schwartz, S. H. (1977). Normative influences on altruism. *Advances in Experimental Social Psychology*, 10, 221–279. [https://doi.org/10.1016/S0065-2601\(08\)60358-5](https://doi.org/10.1016/S0065-2601(08)60358-5)
- Shava, E., & Mazenda, A. (2021). Ethics in South African public administration: a critical review. *International Journal of Management Practice*, 14(3), 306–324. <https://doi.org/doi.org/10.1504/IJMP.2021.115107>
- Sherif, E., Furnell, S., & Clarke, N. (2015). An identification of variables influencing the establishment of information security culture. *International Conference on Human-Computer Interaction and Lecture Notes in Bioinformatics*, 436–448. https://doi.org/10.1007/978-3-319-20376-8_39
- Shih, S. P., & Liou, J. Y. (2015). Investigate the effects of information security climate and psychological ownership on information security policy compliance. *Pacific Asia Conference on Information Systems, PACIS 2015 - Proceedings*, 28. <https://aisel.aisnet.org/pacis2015/28>
- Simon, J. (2014). A Self-Regulatory Approach to Behavioral Compliance with IS Security Policies – “Come on, Baby, do the Locomotion.” *AMCIS 2014 Proceedings*, 1–11. Association for Information Systems. <https://aisel.aisnet.org/amcis2014/Posters/ISSecurity/32>
- Siponen, M., Pahlila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An empirical investigation. *IEEE Computer Society*, 43(2), 64–71. <https://doi.org/10.1109/MC.2010.35>

- Siponen, M., Soliman, W., & Vance, A. (2022). Common Misunderstandings of Deterrence Theory in Information Systems Research and Future Research Directions. *Data Base for Advances in Information Systems*, 53(1), 25–60. <https://doi.org/10.1145/3514097.3514101>
- Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee Information Systems Security Policy Violations. *Nature*, 34(3), 487–502. <https://doi.org/10.1038/174197b0>
- Smita Verma. (2025). Cybersecurity compliance in the age of remote work: Challenges and solutions. *World Journal of Advanced Engineering Technology and Sciences*, 15(1), 1112–1120. <https://doi.org/10.30574/wjaets.2025.15.1.0286>
- Sohrabi, N., Maple, C., Furnell, S., & Ajmal, M. (2019). Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Generation Computer Systems*, 97, 587–597. <https://doi.org/10.1016/j.future.2019.03.024>
- Solomon, G., & Brown, I. (2020). The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management*, 34(4), 1203–1228. <https://doi.org/10.1108/JEIM-08-2019-0217>
- Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management and Computer Security*, 22(1), 42–75. <https://doi.org/10.1108/IMCS-08-2012-0045>
- Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information and Computer Security*, 23(2), 200–217. <https://doi.org/10.1108/ICS-04-2014-0025>
- Sommestad, T., Karlzén, H., & Hallberg, J. (2019). The Theory of Planned Behavior and Information Security Policy Compliance. *Journal of Computer Information Systems*, 59(4), 344–353. <https://doi.org/10.1080/08874417.2017.1368421>
- Son, J. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, 48(7), 296–302. <https://doi.org/10.1016/j.im.2011.07.002>
- Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information and Computer Security*, 25(5), 494–534. <https://doi.org/10.1108/ICS-07-2016-0054>
- Topa, I., & Karyda, M. (2015). Identifying factors that influence employees' security behavior for enhancing ISP compliance. *International Conference on Trust and Privacy in Digital Business*, 9264, 169–179. https://doi.org/10.1007/978-3-319-22906-5_13

- Toyana, M. (2021, September 9). Cyber bandits target South Africa: Department of Justice Space Agency hit by ransomware attacks. *Daily Maverick*.
<https://www.dailymaverick.co.za/article/2021-09-09-cyber-bandits-target-south-africa-department-of-justice-space-agency-hit-by-ransomware-attacks/>
- Trafimow, D. (2009). The Theory of Reasoned Action: A Case Study of Falsification in Psychology. *Theory & Psychology*, 19(4), 501–518.
<https://doi.org/10.1177/0959354309336319>
- Trarynny, I. (2025). *2025 Data Breach Prevention Strategy Guide*.
<https://www.feroot.com/blog/colorado-privacy-act-cpa-compliance-feroot/>
- Vadisetty, R. (2024). The Effects of Cyber Security Attacks on Data Integrity in AI. *International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)*, 1–6. <https://doi.org/10.1109/ICEC59683.2024.10837148>
- Valencia, G. (2022). *A Correlation Analysis of Organizational Commitment and Support toward ISP Compliance Intention*. Capella University.
<https://www.proquest.com/openview/4239178d2b7ac35f7c822fb6d5378e2e/1?pq-origsite=gscholar&cbl=18750&diss=y>
- Wang, X., Wang, C., Sun, Z., & Wang, C. (2023). An optimal coupling incentive mechanism concerning insider's compliance behavior towards marine information security policy. *Journal of Ocean Engineering and Science*, 8(5), 573–575.
<https://doi.org/10.1016/j.joes.2022.05.023>
- Wang, X., & Xu, J. (2021). Deterrence and leadership factors: Which are important for information security policy compliance in the hotel industry. *Tourism Management*, 84.
<https://doi.org/10.1016/j.tourman.2021.104282>
- Wiafe, I., Koranteng, F. N., Wiafe, A., Obeng, E. N., & Yaokumah, W. (2020). The role of norms in information security policy compliance. *Information and Computer Security*, 28(5), 743–761. <https://doi.org/10.1108/ICS-08-2019-0095>
- Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 37(1), 1–20. <https://doi.org/10.25300/MISQ/2013/37.1.01>
- Wu, R., Ahn, G.-J., & Hu, H. (2012). Towards HIPAA-compliant healthcare systems. *Proceedings of the 2nd ACM SIGHIT Symposium on International Health Informatics - IHI '12*, 593.
<https://doi.org/10.1145/2110363.2110429>
- Xue, B., Xu, F., Luo, X., & Warkentin, M. (2021). Ethical leadership and employee information security policy (ISP) violation: exploring dual-mediation paths. *Organizational Cybersecurity Journal: Practice, Process and People*, 1(1), 5–23. <https://doi.org/10.1108/ocj-02-2021-0002>

- Yazdanmehr, A., Jawad, M., Benbunan-Fich, R., & Wang, J. (2024). The role of ethical climates in employee information security policy violations. *Decision Support Systems*, 177. <https://doi.org/10.1016/j.dss.2023.114086>
- Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, 92, 36–46. <https://doi.org/10.1016/j.dss.2016.09.009>
- Yin, R. K. (2003). *Case Study Research Design and Methods* (3rd ed., Vol. 5, Issue 3). Sage Publications. https://doi.org/10.1300/J145v03n03_07
- Zahle, J. (2025). Bias and debiasing strategies in qualitative data collection. *Philosophy of Science*, 92(3), 606–623. <https://doi.org/10.1017/psa.2024.70>

8. LIST OF APPENDICES

8.1 APPENDIX A: LIST OF FACTORS

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
1.	(Bauer Bernroider, 2017)	&To investigate whether individual behavioural compliance with the ISP is influenced by accumulated security information and information security awareness.	Theory of reasoned action	Attitude towards information security compliance	Banking environment	√		√	√
	(Cannoy Salam, 2010)	&To present a framework of Information Assurance and Compliance developed through multi-site case study approach involving multiple health care providers in the U.S.	Theory of reasoned action	Individual propensity for compliance Government regulations Organizational culture competency Training on IS policies Communication of policies Training on IS technology Previous experience with IS technology	Health sector in the US	√			

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
				Management commitment Rewards and punishment Perceived ease of use of IS technology					
2	(Cheng et al., 2013)	To explore the influence of formal and informal control on ISP violations intentions	Social bond Deterrence	Perceived severity of beliefs Social pressure- co-worker behaviour	10 organizations in China				
3	(Siponen et al., 2010)	To determine the causes of non-compliance to ISP	Protection motivation Deterrence Reasoned action Innovation diffusion	Normative belief Threat appraisal (Perceived vulnerability and perceived severity and celerity) Self-efficacy Visibility Deterrence Social pressure Awareness of ISP	Private sector organizations				
4	(Bulgurcu et al., 2009)	To identify the factors that drive an employee to comply with	Theory of Planned Behaviour Social Identity	Information security awareness Work experience	Diverse set of organizations				

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
		requirements of the ISP.		Training incentives					
5	(Yazdanmehr & Wang, 2016)	To propose a model to examine how ISP related norms and activators to affect employees ISP Compliance behaviour	Norm activation theory Social norms theory	Awareness of consequences Ascription of personal responsibility ISP –related personal norms	Diverse set of organizations in the USA	√	√		
6	(Li et al., 2014)	To propose a framework to compare two distinct approaches for achieving compliance	Deterrence theory Organizational justice theory	Self –regulatory forces Personal ethics Organizational justice beliefs(distributive ,procedural and informational justice) Sanction mechanisms(sanction certainty)	Diverse set of organizations in the USA				
7	(Choi, 2017)	To provide a unique framework for understanding the influence of HRM practices on individual security policy compliance outcomes.	Social exchange theory	Developmental-oriented appraisal externally or internally Equitable reward, selective staffing and training	Diverse banks in Korea	√			
8	(Siponen, 2010)	To develop an IS security program that is theoretically and empirically grounded	Universal constructive instructional theory Elaboration likelihood model	Training and education	Small organization in Finland				

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
9	(Alfawaz et al., 2010)	To identify factors that influence information security behaviour	Theory of reasoned action/Theory of planned behaviour	Organizational cultural values Top management commitment Training and skills Security awareness programs Organizational IT structure Appointment of information security managers Motivation system	Organizations in Saudi Arabia				
10	(Nasir et al., 2017)	To propose a conceptual framework of ISP compliance behaviour based on new proposed ISC dimensions	Theory of planned behaviour	Procedural countermeasures (information security awareness) Top management commitment Information security knowledge sharing Security knowledge	Universal	√			

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
				Information security training and education Information security risk management Monitoring (tracking computing activities and performing security audits) Attitude Self-efficacy Normative belief					
11.	(Al-Omari et al., 2013)	To investigate the role of ethics in explaining information security compliance	Theory of planned behaviour Ethics theory	Attitudes Subjective norms Self-efficacy Moral obligation Formalism	Seven banks in Jordan				
12.	(Bulgurcu et al., 2010)	To identify rationality based factors rooted in the rational theory	Theory of planned behaviour Rational choice theory	Attitude towards compliance Normative beliefs Self-efficacy Benefit of compliance	Diverse set of organizations in USA				

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
				Cost of compliance Cost of non-compliance Information security awareness					
14.	(Siponen & Vance, 2010)	To propose a theoretical model to test the effects of neutralization and sanctions	Neutralization theory Deterrence theory	Use of neutralization techniques	Three organizations in Finland (a university, an electrical company and a large supermarket)				
15.	(Bauer et al., 2017)	To address the challenge of IS management in banks , to design ISA programs and explores how users perceive program designs embedded in organization settings	Neutralization theory	Perceived knowledge of ISP Perceived importance of ISP Perceived responsibilities regarding ISP Use of neutralization techniques Perceived IS risks	Three banks in Europe				
16.	(Sohrabi Safa et al., 2016)	To present a conceptual framework that shows how information security compliance arises in organizations.	Social Bond Theory Involvement Theory	Information security knowledge sharing Collaboration Intervention Experience	Four companies in Malaysia	√	√		

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
				Information security awareness Commitment Involvement Personal belief Attitude towards compliance					
17.	(Lowry & Moody, 2015)	To develop an innovative model that uses an integrated model to examine two counterpoised forces to predict intent to comply with new ISP's in organizations	Organizational control theory Reactance theory	New ISP mandatories Existing organizational formal controls Threats to personal freedom	Industry participants from a several key industries				
18.	(Al-Omari et al., 2012)	To develop a measurement tool that provides better measures for predicting and explaining employees' compliance with ISP's by examining the role of information security awareness in enhancing employees' compliance to ISP.	Theory of planned behaviour	Information security awareness Perceived usefulness Perceived ease of use	Banking environment in Jordan				

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
19.	(M. Choi & Song, 2018)	To investigate factors that affect individual perception of sanctions threat	Social control /social bond theory	Commitment Belief Attachment	Public institutions in Korea				
20.	(Milicevic & Goeken, 2013)	To analyse existing empirical research findings on ISP compliance and suggest a presentation format that may allow ISS practitioners to base their ISP design on	N/A	Attitude Subjective norms Certainty of detection Normative beliefs Self-efficacy Descriptive norm Information quality Openness to change Peer behaviour Perceived effectiveness Preventional reasoning Response efficacy Social influence Social trust	Literature analysis				
21	(D'Arcy et al., 2009)	To introduce and empirically test an	General deterrence model	User awareness of security policies	Eight organizations in the US				

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
		extended GDT model that posits that user awareness of security countermeasures directly impacts user perceptions of the certainty and severity of sanctions associated with IS misuse ³		Security education, training and awareness Computer monitoring					
	(Mavetera et al., 2015)	To investigate the compliance of staff to the information security policy within a municipality	None	Information security policy awareness Information security knowledge	Municipality in South Africa			√	√
22.	(Johnston et al., 2015)	To propose an enhanced fear appeal rhetoric framework to represent the impact of fear appeal and sanction elements on information security policy compliance intentions	Protection motivation theory	Sanctioning rhetoric Informal sanction severity Informal sanction certainty Perceived threat severity Perceived threat susceptibility Perceived self-efficacy	Finish City Government	√		√	
23.	(Mani et al., 2015)	To investigate the factors that influence real estate employees	Protection motivation theory	Perceived vulnerability Perceived severity	Real estate businesses in Australia				

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
		intended information security behaviour		Previous incidents Response efficacy					
24.	(X. Chen & Chen, 2018)	To propose research model based on the Awareness-Motivation-Capability framework to unify the factors to predict employees' ISP compliance intention	Theory of planned behaviour General deterrence theory Protection motivation theory Rational choice theory	Perception of controllability Self-efficacy Capability Cost to comply with ISP Reward Penalty severity Motivation ISP Awareness Awareness of the seriousness of security threats Awareness of the importance of information security	Mid-size regional university in the northwest of the USA				
25	(Padayachee, 2012)	To classify various factors that motivate or negate compliant security behaviour in order to alert organizations to	Self-determination theory Deterrence theory Contemporary deterrence theory	Awareness Normative beliefs Threat appraisal Self-efficacy	Literature studies				

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end users compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
		the strategies that are most effective?	Protection motivation theory	Response efficacy Visibility Deterrence Social disapproval Self-disapproval Organizational commitment Rewards Social climate Coping appraisal Threat appraisals Sanctions Deterrent controls					
26	(Stewart & Jürjens, 2017)	To address the lack of research evidence on what influences information security management development and implementation	Social Bond theory	Poor information security awareness Poor information security training Poorly managed teams Unskilled management boards	Different organizations in Germany	✓	✓		

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
				Information security risk management Absence of compliance policy Hardware failures					
27	(Herath & Rao, 2009)	To develop and test an integrated protection Motivation and Deterrence model of security policy compliance	Theory of Planned behaviour Protection Motivation Theory Deterrence Theory	Perceived severity of potential security breach High level of security breach concern Perceived effectiveness of user's actions Resource availability Perceived response cost Self-efficacy Normative beliefs Certainty of detection Subjective norms Descriptive norms Level of organizational commitment	Several organizations in western New York	√	√		
28	(Ifinedo, 2017)	To investigate employees' information systems security policy (ISSP)	Theory of Planned behaviour Social bond theory	Employees' perceptions of IS security threats Commitment	Canadian organizations	√	√		

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
		compliance behavioural intentions	Protection motivation theory	Involvement Attachment Personal norms Attitude towards ISSP compliance					
	(Son, 2011)	To offer a theoretical explanation for why employees do or do not follow their organization's ISSP	General deterrence theory	Perceived legitimacy Perceived value congruence	Various organizations in the united States				
29	(Hedström et al., 2011)	To investigate user compliance and security practices as part of people's everyday activities	Theory on organizational learning Social action theory	Value conflicts (between management and users)	(Health care facilities in Sweden				
30	(Sommestad et al., 2014)	To present a systematic review of empirically supported research findings in order to determine important variables for security compliance	Not specified	Perceived justice of punishment Perceived legitimacy Threat appraisal Information security awareness Descriptive norm Information security policy fairness	Literature studies				

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end users compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
				Normative beliefs Perceived value congruence					
31	(Nasir et al., 2019)	To propose an information security culture model to examine its influence on employees' information security policy compliance	Organizational culture	Attitude Normative belief Self-efficacy Information security culture	Universities in Malaysia	√	√		
32	(Sohrabi et al., 2019)	To investigate the effect of sanction certainty and severity as deterrent factors and the effect of increasing the effort and risk reducing the rewards and provocations, and removing excuses as situational crime prevention factors on employees' attitude towards preventing misbehaviour in the domain of information security	General deterrence theory Situational crime prevention theory Theory of planned behaviour	Perceived sanction severity Perceived sanction certainty Increasing the effort for information security misconduct Increasing the risk for information security misconduct Reduce the rewards for information security misconduct Attitude Perceived behavioural control	Several organizations in the UK in the banking e-Commerce and education	√			

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
				Subjective norms towards intention to secure information Intention to protect information behaviour					
33	(Rajab & Eydgahi, 2019)	To present a comprehensive theoretical model for predicting intentions of higher education employees' compliance with information security policies.	Protection motivation theory Theory of planned behaviour General deterrence theory Organizational theory	Perceived vulnerability Response efficacy Response cost	University in Midwest of the United states				
34	(Foth, 2017)	To identify the most significant factors influencing employees intention to comply with data protection regulations	Theory of Planned behaviour General Deterrence theory	Attitude Subjective norms Perceived behavioural control Detection certainty	Hospitals in Germany	✓			
35	(X. Chen et al., 2018)	To integrate various theories to form a broad view of employee security policy compliance	Deterrence theory Penalty Protection motivation theory Theory of planned behaviour	Capability Self-efficacy Perception of controllability Awareness	Mid-size regional university in the northwest of the USA				

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
			General deterrence theory						
36	(Hina et al., 2019)	To integrate factors from two validated theories with institutional governance (IG) factors to investigate the contribution of IG factors in promoting the protection behaviour of employees	Protection motivation theory Theory of planned behaviour	Attitude Perceived behavioural control Perceived severity perceived vulnerability Self-efficacy SETA programs Provision of ISPs Negative experience	Higher education institutions in Malaysia				
37	(Li et al., 2019)	To investigate the relationship of PMT influences of safety behaviour , organizational social influence, and organizational calls to action on employees information security behaviours	Protection motivation theory	Peer behaviour Cues to action Prior experience Response efficacy Self-efficacy Perceived vulnerability	Various organizations in the US	√	√		
38	(Sommestad, Karlzén, Hallberg, et al., 2019)	To test whether there are variables that improve the predictions of security policy	Theory of planned behaviour	Information security policy awareness Anticipated regret	Literature studies				

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
		compliance behaviour when added to a prediction model after the variable of the theory of planned behaviour		User involvement in information security work Organization's information security capability					
39	(Chen & Li, 2019)	To investigate employees' extrarole behaviour in the security context based on person-organization fit theory	Person organization fit theory	Perceived demand-ability fit Perceived need –supply fit Security commitment	IT and finance Organizations in China				
40	(Alzahrani, 2021)	To analyse the impact of organisational security factors and individual non-compliance on users' intentions towards information security policies.	Not specified	Size of the organization Peer behaviour Security education Work impairments Employees' anxiety Security visibility Top management's commitment and participation	Educational organization in Saudi Arabia				

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
				Information security awareness training Continued communication processes					
41	(Karim et al., 2021)	To investigate factors that influence compliance behaviour of information security policy in a public sector agency.	Theory of planned behaviour, Rational choice theory Innovation diffusion theory	Educational level Fear appeal Attitude Normative belief Individual's dominant decision style Involvement Beliefs Collaboration between employees, Knowledge Sharing Perceived Cost of Noncompliance Perceived Cost of Compliance	Government agency in Malasia			√	
42	(Palanisamy et al., 2020)	To identify the unique features of	None	Threat severity	Literature review				

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
		BYOD in organizations To present theories used in previous BYOD security policy compliance studies; To identify factors that influence security policy compliance; To Identify limitations and open research issues.		Self-efficacy Response cost Response efficacy					
43	(Wang & Xu, 2021)	To examine how deterrence perception and managers' leadership influence employees' intention to comply with information security policies	Dual-process theories of information processing Deterrence theory	Perceived deterrent certainty Ethical leadership	Chinese hotel				
44	(Alassaf & Alkhalifah, 2021)	provides a systematic literature review synthesizing the psychological theories, organizational	Not specified	Information security education, training and Awareness Trust Leadership	Literature review				

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
		theories, and other internal and external factors on information security policy compliance researches		Security related stress Understanding resource vulnerability Moral beliefs Organizational citizenship behaviours Organizational deviance Perceived organizational formalization Work related groups Ethical climate Organization's information security Information security education, training and Awareness Trust Security related stress Understanding resource vulnerability Moral beliefs					

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
				Organization's information security strategy access Position level Satisfaction Confirmation Security avoidance Participation in decision making Demographic Corporate social responsibility SETA programs Psychological empowerment Religiosity Supportive organizational culture Internal audit Behavioural monitoring Provision of policy					

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
				Negative experience Security agents Informational materials Compliance audit National culture Worries about cyber crime Working experience Self-regulatory approach Psychological ownership Organizational injustice.					
45	(Nasir et al., 2020)	To discuss a pilot study of research-in-progress that proposes a holistic ISC model to be used as guidance for employee's security behaviour in organization.	Theory of planned behaviour	Attitude Normative belief	Malaysian public university				
46	(Liu et al., 2020)	To investigate the influence of supervisor-supervisor-	Technology threat avoidance theory	Supervisor-subordinate guanxi	Chinese Government			√	

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end users' compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
		subordinate guanxi (SSG) and organizational commitment in the information security management To identify key factors that motivate government employees' ISP compliance in the Chinese context	Social exchange theory Chinese Government	Organizational commitment					
47	(Ali, Dominic, Emad, et al., 2021)	To determine employees' noncompliance behaviour's transformation steps to compliance behaviour to develop a process model	Not specified	Information security awareness, culture, and management Protection motivation behaviours Fear appeal Information Security Knowledge sharing Self-efficacy Response efficacy Attitude towards compliance Perceived vulnerability Maladaptive rewards	Literature review				

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
				Psychological capital Psychological ownership Organizational citizenship Security responsibility Perceived effect Response cost Self-morality Fear appeal Social influence Subjective norms Past behaviour(habit) Perceived threat severity Perceived threat susceptibility Coping appraisal Organization criticality Perceived impact Security culture					

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
				Job satisfaction Organizational norms Moral obligation Leadership Management Security awareness Training Levels of ISP knowledge Organizational behaviour Threat appraisal Organizational security policy Psychological contract Employees' status (hierarchal rank) Moral corporate social responsibility Rational choice theory factors					

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
				Information security monitoring Computer monitoring Social learning factors Employment status Organizational inertia Individual inertia Belief Values Supervisor's support Extra role behaviours In role behaviours ISP related personal norms Social bonding with an extending view of involvement Situational Crime Prevention Theory (SCPT) and Social Bond Theory (SBT) components					

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
				Person organization fit Good organizational governance perceived behavioural control subjective norms Organizational commitment					
48	(Ali et al., 2020)	To provide a comprehensive framework for information security policy compliance (ISPC) for the O&G sector	Social bond theory	SETA programs Attachment Commitment Involvement Personal norms	Oil and gas industry in developing countries, focusing on Malaysia	√	√		
49	(Amankwa et al., 2022)	To examine the individual and combined effects of organisational and behavioural factors on employees' attitudes and intentions to establish an information security policy compliance culture in organisations.	Accountability Theory Organisational culture theory, Social bond theory	Supportive organizational culture User involvement Employees Attitude Organizational culture Awareness of IS Monitoring	Ghanaian organisations that had institutionalised ISP(Financial services, Telecommunication, education hospitality, healthcare, agriculture, mining, entertainment, manufacturing and oil and gas)	√			

No	Article /Study	Purpose of the research/contribution	Theory	Identified factors affecting end user compliance	Focus area/environment	Framework developed	Framework validated	Government department	SA
50	(Karlsson et al., 2022)	To investigate the connection between different perceived organizational cultures and information security policy compliance among white-collar workers.	None	Organizational culture	White-Collar workers in Sweden				
TOTAL						16	8	5	2

8.3 APPENDIX B: ETHICS APPROVAL



College of Science, Engineering and Technology_ School of Computing_ERC

Date: 12/02/2026

Dear: Ms Sakhile Charity Dories Lekhuleni

**Decision: Ethics Approval from
12/02/2026 to 12/02/2029**

NHREC Registration # : (if applicable)
Ref #: 2036
Name: Ms Sakhile Charity Dories Lekhuleni
Student #: 34906592
Staff #:

Researcher: Ms Sakhile Charity Dories Lekhuleni

Corner of Christiaan de Wet Road & Pioneer Avenue, Florida

Johannesburg

Email address: 34906592@mylife.unisa.ac.za

Supervisor: Prof Adele da Veiga dveiga@unisa.ac.za

A Framework for End-User Compliance with the Information Security Policy in Government Institutions

Qualification: Masters in Computing

Thank you for the application for research ethics approval by the College of Science, Engineering and Technology_ School of Computing_ERC for the above-mentioned research study. Ethics approval is granted for three years.

The low risk application was reviewed by the College of Science, Engineering and Technology_ School of Computing_ERC on 14/02/2024 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment.

The proposed research may now commence with the provisions that:

1. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
2. Any adverse circumstance arising during the undertaking of the research study that may affect the ethical integrity of the study, including those involving research participants, third parties, or juristic persons, must be reported in writing to the College of Science, Engineering and Technology_ School of Computing_ERC without delay.
3. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
4. Any changes that may affect study-related risks to research participants, juristic or third persons, must be reported in writing to the College of Science, Engineering and Technology_ School of Computing_ERC, accompanied by a progress report.

5. The researcher will ensure that the research study complies with all applicable national legislation, professional codes of conduct, institutional guidelines, and scientific standards relevant to the specific field of study. Where applicable, adherence to the following South African legislation is essential: the Protection of Personal Information Act (No. 4 of 2013), the Children's Act (No. 38 of 2005), and the National Health Act (No. 61 of 2003)
6. Future use of this research data is permitted only in de-identified form and only for secondary research with objectives similar to those of the original study. Any secondary use involving identifiable human data will require additional ethics clearance.
7. No fieldwork activities may continue beyond the stated expiry date 12/02/2029. A completed Research Ethics Progress Report must be submitted as an application for renewal and is subject to approval by the Research Ethics Committee. A Close-Out Report must be submitted upon completion of the research study.
8. The College of Science, Engineering and Technology_ School of Computing_ERC may require the submission of regular progress reports on an annual basis, in alignment with Section 7.2 of the Unisa Policy on Research Ethics (2024).

Additional Conditions

1. Disclosure of data to third parties is prohibited without explicit consent from the research participants and Unisa.
2. Research data must be stored in compliance with the university's research data management policy for a period of up to 15 years.
3. When publishing the results, the researcher must take appropriate precautions to safeguard the confidentiality and privacy of the research participants, juristic persons, third parties, and the university, in accordance with institutional policies and ethical standards.
4. Adherence to the National Statement on Ethical Research and Publication Practices, specifically Principle 7 on Social Awareness, must be ensured. This principle states: 'Researchers and institutions must be sensitive to the potential impact of their research on society, marginal groups, or individuals, and must consider these when weighing the benefits of the research against any harmful effects, with a view to minimising or avoiding the latter where possible.' The University of South Africa (Unisa) accepts no liability for any failure to comply with this principle.

Note

The reference number 2036 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.

Kind regards,



Prof. L. Motsi

Chair of College of Science, Engineering and Technology_ School of Computing_ERC
E-mail: motsil@unisa.ac.za



Prof. I. Naidoo

Executive Dean / By delegation from the Executive Dean of College of Science, Engineering and Technology_ School of Computing_ERC
E-mail: naidoi@unisa.ac.za

8.4 APPENDIX C: PERMISSION LETTERS



Rhino Building, Government Boulevard, Riverside Park, Ext. 2, Mbombela, 1200, Mpumalanga Province
Private Bag X11310, Mbombela, 1200, Mpumalanga Province
Tel I: +27 (13) 766 6761, Fax: +27 (13) 766 8496

Litiko Letemisebenti Yomphakathi,
Ternigwaco Netokutfutso

Departement van Openbare Werke,
Paais en Vervoer

UmNyango wezemiSibenzl yomPhakathi,
zeeNdlela nezokuThutha

MS LEKHUJENI SAKHILE DORIES CHARITY

0184

Dear Madam

SUBJECT: REQUEST FOR APPROVAL TO CONDUCT RESEARCH: yourself

1. Your request to conduct research for academic purposes refers.
2. The Department of Public Works, Roads and Transport hereby grants you permission to conduct research on condition that the findings, information collected and recommendations will be solely used for academic purposes. The researcher should also share the findings of the study with the department.
3. You will be strictly required to adhere to all principles of research ethics and departmental protocols.
4. The image of the department has to be protected at all times.
5. This permission will serve as an access document to participants.
6. The researcher must make findings of the study available to the department.
7. The Department wishes you well in your study.

HEAD: PUBLIC WORKS, ROADS AND TRANSPORT
DATE: 18/9/2023



Ms. SCD Lekhuleni
The Researcher
University of South Africa
Preller Street, Muckleneuk Ridge
City of Tswane
0003

Dear Ms. Lekhuleni

**RE- REQUEST FOR PERMISSION TO CONDUCT RESEARCH AT MPUMALANGA DEPARTMENT OF
COMMUNITY SAFETY, SECURITY AND LIAISON: A FRAMEWORK FOR END-USER INFORMATION
SECURITY POLICY COMPLIANCE IN A GOVERNMENT INSTITUTION**

1. Your request for permission dated 07 March 2023 is hereby acknowledged by the Department.
2. This serves to inform Ms SCD Lekhuleni, a registered student at University of South Africa with student number: **34906592** permission to conduct research at the Mpumalanga Department of Community Safety, Security and Liaison on a Framework for End-User Information Security Policy Compliance in a Government Institution is hereby granted.
3. Hope you will find the above to be in order.

Kind regards,

ACTING HEAD: COMMUNITY SAFETY, SECURITY AND LIAISON

DATE: 18/03/2023



CONSENT TO PARTICIPATE IN THIS STUDY- GOVERNMENT OFFICIAL

STUDY TITLE: A FRAMEWORK FOR END-USER INFORMATION SECURITY

POLICY COMPLIANCE IN GOVERNMENT INSTITUTIONS

I, _____ (participant name), confirm that the researcher, Ms SCD Lekhuleni has informed me about the nature, procedure, potential benefits and anticipated inconvenience of participation in the study.

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.

I agree to the recording of the interview during the data collection process.

I have received a signed copy of the informed consent agreement.

Participant Name & Surname..... (please print)

Participant Signature..... Date 26/ 03/2024

Researcher's Name & Surname.....Sakhile Lekhuleni

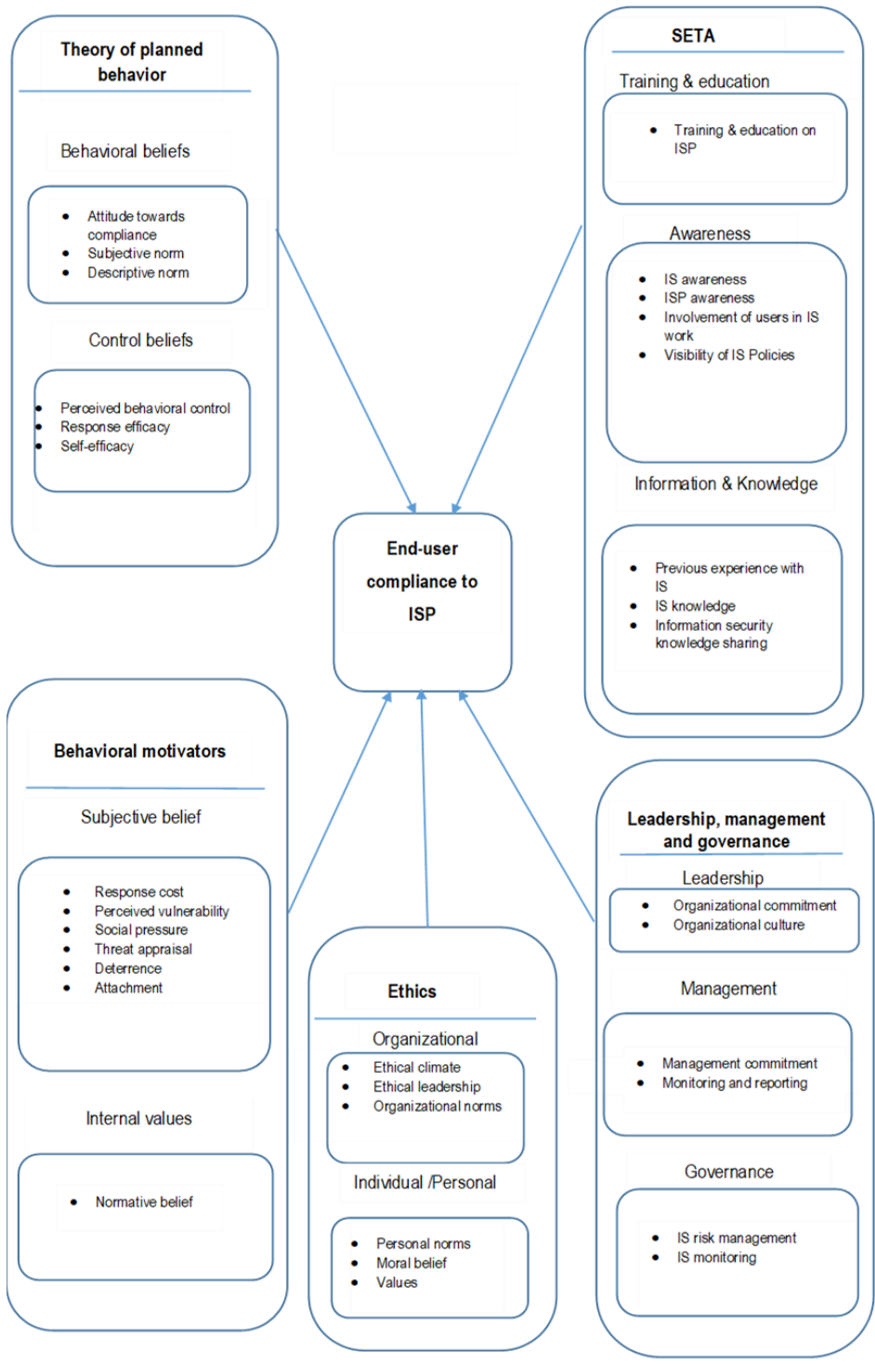
Researcher's signature..... Date.....



University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

8.6 APPENDIX E: INTERVIEW GUIDE -GOVERNMENT OFFICIALS

PROPOSED ECISP FRAMEWORK



The diagram above depicts the model of the proposed EISP Compliance Framework. The model consists of components, which are crucial building blocks of the EISP Compliance framework.

The Model Components are:

- Theory of Planned Behaviour (TPB)
- Behavioural Motivators
- Ethics
- Security Education, Training, and Awareness (SETA):
- Leadership, Management, and Governance

Each of these components consists of factors that have been identified through literature review, highlighting their impact on end-user compliance with Information Security Policy in government institutions.

The integration of these components and their respective factors forms the building blocks of the proposed EISP Compliance framework. The framework aims to provide a holistic approach to enhance end-user compliance with Information Security Policy.

INTERVIEW QUESTIONS

The purpose of these interview questions is to confirm whether the components and factors of the proposed EISP Compliance framework are, suitable, complete and applicable, in improving ISP compliance in a government institution. The output of the interviews with government officials will be used to refine the proposed EISP Compliance framework.

SUITABILITY

1. Considering the context of your government institution, do you believe the framework is suitable for its specific needs and requirements?
2. Are there any adjustments or customizations that should be made to better fit the institution's environment?
3. Do you think the components are relevant to improve end-user compliance to information security policy in your institution?
4. Which components of the framework do you consider to be the most suitable for ensuring end-user compliance with information security policy?
5. Please specify if some of the components should be removed, and motivate where necessary
6. Please specify if you would add new components, and motivate where necessary

USABILITY

1. How clear and user-friendly is the framework in guiding end-user compliance with the ISP?
2. If it is not clear, please indicate how the framework can be improved.
3. Are there any areas where the framework can be improved for better understanding?
4. Please indicate whether you believe the proposed framework will be easy to use and apply in your organization.

COMPLETENESS

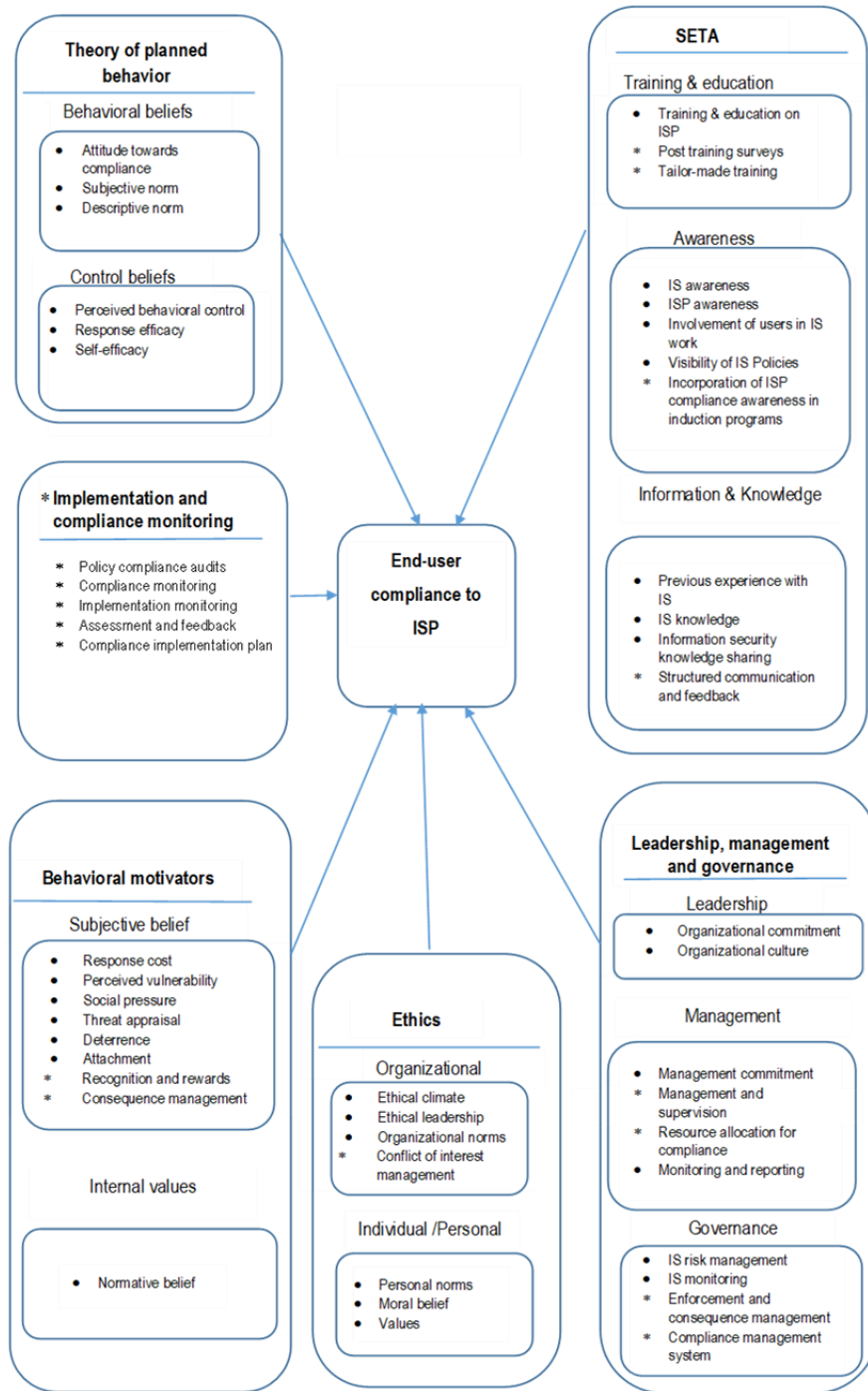
1. Does the framework cover all essential aspects of information security policy compliance that are relevant to the government institution?
2. Are there any key components or elements missing that should be included in the framework?

APPLICABILITY

1. How feasible is it for your organization to implement the proposed framework?
2. How applicable are the individual components in ensuring overall compliance with information security policy in your organization?

8.7 APPENDIX F: INTERVIEW GUIDE-EXPERTS

PREFINED ECISP COMPLIANCE FRAMEWORK



The diagram above depicts the model of the proposed EISP Compliance Framework. The model consists of components, which are crucial building blocks of the EISP Compliance framework.

The Model Components are:

- Theory of Planned Behaviour (TPB)
- Behavioural Motivators
- Ethics
- Security Education, Training, and Awareness (SETA):
- Leadership, Management, and Governance

Each of these components consists of factors that have been identified through literature review, highlighting their impact on end-user compliance with Information Security Policy in government institutions.

The integration of these components and their respective factors forms the building blocks of the proposed EISP Compliance framework. The framework aims to provide a holistic approach to enhance end-user compliance with Information Security Policy.

INTERVIEW QUESTIONS

The purpose of these interview questions is to assess whether the proposed EISP framework is accurate, comprehensive, relevant, and effective in improving end user compliance to ISP in a government institution. The output of this interview will be used to improve the proposed EISP Compliance framework and develop a final EISP Compliance framework.

ACCURACY

1. Are the components of the framework accurately defined and described?
2. How well does the framework align with industry best practices and standards for information security policy compliance?
3. Are there any areas in the framework that might need further clarification or refinement to ensure accuracy?
4. Do you see any potential conflicts or discrepancies between the framework and existing information security policies or regulations?

COMPREHENSIVENESS

1. How well do you think the proposed framework covers all the essential components and factors of end-user compliance to information security policy?
2. Do you believe that the framework is comprehensive enough to improve end-user compliance to ISP? Motivate if possible

-
1. How well do you think the proposed framework covers all the essential components and factors of end-user compliance to information security policy?
 2. Do you believe that the framework is comprehensive enough to improve end-user compliance to ISP? Motivate if possible
 3. If not, what would you add to the framework to improve end-user compliance to ISP? Motivate if possible
 4. Does the framework address the specific needs and challenges of government institutions in terms of information security policy compliance?
 5. Are there any other components that you believe are missing from the framework, or that should be modified or refined?
 6. Any other comments on how to improve the framework?
-

RELEVANCY

-
1. Considering the specific context of government institutions, do you believe the framework is relevant to its needs and requirements?
 2. Does the framework consider the unique challenges and constraints faced by government institutions?
 3. How adaptable is the framework to potential changes in information security practices and policies over time?
-

EFFECTIVENESS

-
1. In your expert opinion, how effective do you think the framework would be in improving end user compliance with information security policy?
 2. What specific components or factors of the framework do you believe would contribute most to its effectiveness?
 3. Based on your experience, are there any potential challenges or limitations that might affect the framework's effectiveness?
-

8.8 APPENDIX G: EMAIL INVITATION

11/7/25, 9:53 PM

Sent Items - LEKHULENI S C D - Outlook



Subject: Request for Consent: Participation in Information Security Policy Compliance Study

From LEKHULENI S C D <34906592@mylife.unisa.ac.za>

Date Wed 2024/03/13 10:03

To [REDACTED]

3 attachments (1 MB)

Appendix D-Participant information sheet Government Officials.pdf; Appendix G-Permission letter DPWRT.pdf; Appendix B-Consent to participate in this study- Government officials.pdf;

Good Morning [REDACTED]

I hope this email finds you well. I am writing to inform you about a research study on information security policy compliance that I am currently conducting through the University of South Africa (UNISA). As you are an ICT employee within the Department of Public works, I am reaching out to request your participation in this study. I have received approval from your Accounting Officer to conduct this research within your organization. Your participation is crucial in contributing to the advancement of knowledge in this area.

Attached to this email, you will find the following documents:

Participant Information Sheet: This document provides detailed information about the purpose of the study potential risks, and benefits. Please review this sheet to gain a comprehensive understanding of the study.

Consent Form: This form seeks your consent to participate. Please read it and complete all sections where required.

Approval Letter: A copy of the approval letter from your Accounting Officer, confirming permission for the study to be conducted within your organization.

Your participation in this study is entirely voluntary, and you have the right to withdraw at any time without any consequences. Your responses will be kept confidential, and your anonymity will be maintained in any reports or publications resulting from this study.

Kindly submit the completed consent form to me via email no later **than Monday, the 18th of March, 2024**. Your prompt cooperation is highly appreciated and will contribute significantly to the success of this research endeavor.

If you have any questions or require further clarification about the study, please do not hesitate to contact me at 0837088604, or by replying to this email
Thank you for considering participating in this important research study. Your cooperation is invaluable, and I look forward to your positive response.

Sakhile Lekhuleni
Masters Candidate
UNISA: School of Computing

<https://outlook.office.com/mail/id/AAQkAGUwNDhkM2UyLTgwNTAINGZiYi1hNmRiLTVjYTc4ZjlkYTlhYwAQAKhieHanc4VDvJn4pplzFn0%3D>

1/2



End-User Compliance with Information Security Policy Framework for Government Departments in South Africa

Sakhile Charity Dories Lekhuleni and Adéle Da Veiga ^(✉)

School of Computing, College of Science, Engineering and Technology,
University of South Africa (UNISA), Florida Campus, Johannesburg, South Africa
dveiga@unisa.ac.za

Abstract. The primary cause of security breaches in private and public organizations is employee non-adherence to information security policies. This research aims to develop a framework for end-user compliance with information security policies in government departments. A consolidated framework that integrates all the factors that influence end-user compliance with information security policies will help organizations and security managers realize all the elements that affect information security compliance. The study applied a systematic literature review using the PRISMA protocol to identify the factors and the components that will contribute to the development of the framework. Subsequently, this enables organizations to tailor their strategies and interventions to address specific challenges, thereby increasing the likelihood of successful end-user compliance with information security policies.

Keywords: information security policy · end-user compliance to information security policy

1 Introduction

Information leakage and policy violations have been experienced by several organizations due to the increase in cyber-attacks and the lack of structured mechanisms for policy compliance and enforcement [1, 2]. Most security breaches in organizations are caused by employee's non-adherence to security policies [3, 4]. Organizations depend on information security policies as guidelines for end-user-acceptable behavior toward protecting the organization's information. Nonetheless, end-user compliance with information security policies is still a challenge, and violations of these policies are very common [5–8]. Employees are regarded as the greatest contributing factor to these violations [7, 9–12]. Moreover, organizations have actioned information security policies to enforce compliance; nonetheless, employee violations of policies are still noticeable [7].

Insider threats and non-compliance with information security policy are regarded as one of the major challenges facing organizations [6]. Since 2020, insider threats have

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
T. Guarda et al. (Eds.): ARTIS 2024, CCIS 2347, pp. 365–377, 2025.
https://doi.org/10.1007/978-3-031-84078-4_25

increased by 44%, with an average annual cost of \$15.4 million [13]. Additionally, the report shows that negligence accounted for 56% of incidents, with an average yearly cost of \$6.6 million [13]. Implementing the right technology does not imply that information is properly secured [3, 14]. Employees who adhere to the information security guidelines and principles are crucial to reinforcing effective information security management [15, 16]. Similarly, employees who do not adhere to security policy requirements are the main threat to organizations determined to safeguard their information technology systems and information [7, 17]. Organizations should transform employees from an information security vulnerability to the first line of information security policy (ISP) compliance defense by implementing a people-centric insider threat management program [13, 18]. Security managers should include compliance and human behavior within the organization's security management procedures [13].

Several studies have identified the factors that influence employee compliance with information security policies [3, 8, 19–21]. While most of the research on information security policy compliance has concentrated on the banking and health sectors, limited attention has been paid to its application within government settings. However, government departments are not immune to data breaches, resulting in the loss of vital information and resources and consequential economic harm [22, 23]. Additionally, South Africa's critical government departments are facing escalating threats from online criminals [22]. A study synthesizing all the factors into a unified framework for enhancing end-user compliance with information security in the South African government has not been found. A consolidated framework integrating all pertinent factors will assist government departments and security managers in realizing the range of influences on information security compliance and subsequently improve end-user compliance.

This paper aims to propose a framework for end-user compliance with information security policy in government departments. The research question that guides this study is, "What elements constitute a framework for end-user information security policy compliance in a government department?" This study is conducted by applying a systematic literature review to identify the factors and the components that will contribute to the development of the framework.

2 Background

2.1 Information Security Policy

ISP is defined as specific and understandable guidelines or a set of principles and strategies used to guide the course of action for security activities [3, 24, 25]. ISPs are documents that define the code of conduct, security measures, and good practices for information technology and human resources [26]. It is further defined as documented, formalized procedures that set out guidelines, roles, and responsibilities that must be adhered to by employees of an organization to safeguard its information technology resources. It specifies the acceptable and non-acceptable use of information resources [11, 27, 28]. Paananen et al. [29] add that an ISP is a document that regulates human actions regarding information security within an organization. ISPs are designed to prevent abuse of information and security breaches by employees [29, 30]. It is proposed by

[24] that the ISP should be specific and understandable to employees. Balozian and Leindner [24] suggest that the effectiveness of ISPs has a direct link to employee compliance. According to [31], the objective of an ISP is to explain the duties and responsibilities of employees concerning information security. Furthermore, [32] suggests that the ISP is used to influence how employees interact with information assets and subsequently encourage positive behavior toward compliance with legislative requirements. While it is essential to develop ISPs, relying solely on the development of policies is not sufficient for information security in organizations [27, 33, 34]. Information security management is evolving from reliance on only technological and policy development solutions to paying attention to how to improve information security by preventing non-compliance and motivating end-users to comply with information security policies [6, 8, 33, 35].

2.2 End-User Compliance with Information Security Policies

Information security policy (ISP) compliance is when employees obey the requirements of an information security policy in a quest to protect the information technology resources of the organization [24, 27]. Information security compliance is also defined as conformance with compulsory security procedures and standards [36]. Several organizations experience behavioral information security incidents caused by employees [28, 37, 38]. As a result, insider threats and non-compliance with information security policies have been regarded as one of the major challenges organizations face [39–42].

2.3 The Importance of End-User Compliance to Information Security Policies

Many organizations invest in information security. However, they continue to experience challenges of data breaches and loss of information [37, 43, 44]. Most organizations focus on technological and procedural security measures; however, relying solely on these measures is insufficient to address the challenges of information security breaches [27, 45]. Furthermore, organizations develop information security policies but fail to ensure the implementation of the policies by employees [6]. Organizations need to increase end-user compliance with ISPs in order to protect organizational information and systems from insiders [45].

It is highlighted that existing employees are the primary source of security incidents in organizations, with a 13% increase compared to 2016 [46]. Likewise [47] found that 59% of organizations encountered significant cybersecurity incidents within the preceding year. Organizations remain exposed to financial and reputational losses due to the potential loss of information stored in their information systems. Information security incidents not only result in the loss of critical organizational data but also inflict brand damage and undermine competitive advantages for organizations [48].

It is important to highlight that if employees fail to adhere to ISPs, organizations are exposed to the risk of losing critical information and financial assets. Consequently, information security management and ISP compliance have been regarded as one of the key strategic concerns in organizations [14, 43, 49–51]. The significance of end-user compliance in enhancing information security in organizations is undeniable. Developing good policies is futile if users do not comply with those policies. Ensuring compliance with information security policies is equally important as having technical solutions at

hand [6]. End-user compliance with ISP is key to the success of information security programs of an organization[49, 52].

Most research that was conducted on information security policy compliance was focusing on the banking and health sectors, few studies have been done on information security policy (ISP) compliance in government. Government departments are also experiencing data breaches that lead to the loss of critical information and resources and cause economic damage [22, 23]. Furthermore, online criminals are increasingly targeting some of South Africa's most crucial government departments [22].

3 Research Methodology

The literature review was conducted using the systematic literature review method to determine studies published on end-user compliance with information security policies. [53, 54]. The PRISMA (Proffered Reporting Items for Systematic reviews and Meta-Analyses) protocol for retrieving, screening, and reviewing the retrieved research papers [55] was applied. A systematic literature review (SLR) is a structured process and methodical approach to reviewing and synthesizing research literature on a specific topic. It aims to provide a comprehensive summary of the existing research by following a predefined research strategy [53]. Kitchenham [53], and Furlan [56] describe the stages of the process for conducting a systematic literature review as follows:

- Stage 1: Formulating the research question - the first step involves clearly defining the research question or hypothesis.
- Stage 2: Developing a protocol - researchers create a protocol that outlines the methodology, including the criteria for selecting studies, search strategies, and data extraction methods.
- Stage 3: Literature search - the literature search involves systematically searching various databases and sources to identify relevant studies.
- Stage 4: Screening and selection - the initial search results are screened to remove duplicates and irrelevant studies.
- Stage 5: Data extraction - for the selected studies, researchers extract relevant data using a standardized data extraction form.
- Stage 6: Quality assessment - researchers assess the quality and validity of the included studies using specific criteria or checklists.
- Stage 7: Data synthesis and analysis - the extracted data are synthesized and analyzed to answer the research question.
- Stage 8: Reporting and interpretation - the final stage involves reporting the findings of the SLR in a clear and structured manner.

4 Results

4.1 Status of End-User Compliance with Information Security Policies

Eighty-nine papers were included in the final literature review to address the main research question, "What elements constitute a framework for end-user information security policy compliance in government departments?". Most of the studies related to

end-user compliance with ISPs were not conducted in South Africa. Out of the 89 studies that were analyzed in this research, only two studies were conducted in South Africa. Notably, Bauer & Bernroider [57] developed a framework, albeit unvalidated, and their study did not focus on government departments. Conversely, the study conducted by Mavetera et al. [58] focused on a South African government institution; however, they did not formulate a framework. Most of the ISP compliance studies focus on examining diverse organizations, with a secondary emphasis on the banking sector and higher education institutions. Only five studies specifically targeted government departments [7, 57–60]. Some of the studies address improving end-user compliance with ISPs without developing a framework. Nineteen studies developed a framework of which ten proceeded to validate their frameworks, each study applying different elements, factors and concepts in their frameworks. The researchers of this study applied qualitative analysis to the papers to extract the various elements, factors and concepts in themes and sub-themes, thereby providing a holistic list of the elements that influence end-user compliance to ISPs.

Based on the analysis of the papers, five main themes were identified, namely, the theory of planned behavior, leadership management and governance, behavioral motivators, security education, and training. From the review, it was evident that the theory of planned behavior was used in most of the studies, and therefore, it is added as a main theme. Factors identified within the literature were grouped according to the themes and structured further in sub-themes based on their conceptual alignment and theoretical underpinnings. The themes and sub-themes were used as components of the proposed framework. Table 2 presents the themes and sub-themes identified from the selected literature sources that influence end-user compliance with ISPs (Table 1).

Table 1. Summary of databases searched

Database	#Records identified	#Records after duplicates removed	#Records screened	#Records excluded	#Full-text articles assessed for eligibility
Google Scholar	84	66	66	5	22
IEEE Explore	199	117	117	52	21
ACM	9	7	7	1	3
Web of Science	13	10	10	2	8
Scopus	325	198	198	78	20
Science Direct	35	23	23	3	15
Total	665	421	421	141	89

Table 2. Themes and sub-themes (factors) influencing end-user compliance with ISP.

Main themes	Sub-themes: Factors influencing end-user compliance with ISP
Theory of Planned Behavior	Behavioral beliefs: • Attitude towards compliance [8, 27, 37] • Subjective norm [5, 43, 61–63] • Descriptive norm [61, 62, 64] Control Beliefs: • Perceived behavioral control [26, 63, 65] • Self-efficacy [5, 26, 27, 43, 61, 62, 66–72] • Response efficacy [10, 61]
Behavioral Motivators	Subjective beliefs: • Response cost [70, 73, 74] • Perceived vulnerability [10, 26, 73, 75, 76] • Social pressure [5, 41, 77, 78] • Threat appraisal [5, 66, 69, 79] • Deterrence [41, 69, 80] • Attachment [8, 76, 78, 81] Internal values: • Normative belief [27, 51, 60, 61, 66, 67, 69, 71, 79]
Security Education, Training and Awareness	Training and education: • Training and education on ISP [3, 5, 14, 3, 5, 14, 16, 49, 66, 67, 82–84] Awareness: • IS awareness [5, 8, 16, 27, 51, 52, 67, 79] • ISP awareness [66, 68, 70, 85] Information and knowledge: • IS knowledge sharing [8, 60, 67] • Previous experience with IS [8, 26]
Leadership, Management and Governance	Leadership: • Organizational commitment [5, 7, 62, 69] • Organizational culture [14, 49, 71] Management: • Management commitment [14, 67, 83] Governance: • IS risk management [86–88] • IS monitoring [49, 71, 76]
Ethics	Organisational: • Ethical climate [49] • Ethical leadership [89] • Organizational norms [5] Individual/personal: • Personal norms [76] • Moral belief [49] • Values [5]

4.2 The Conceptual Framework: End-User Compliance with Information Security Policy Framework

The End-User Compliance with Information Security Policy Framework, which will help enhance end-user compliance with ISPs in government departments, is depicted in Fig. 1. The factors used to develop the framework are based on the main and sub-themes derived from the literature review, as summarized in Table 2. The conceptual framework illustrates the relationships between the factors and end-user compliance with information security policies.

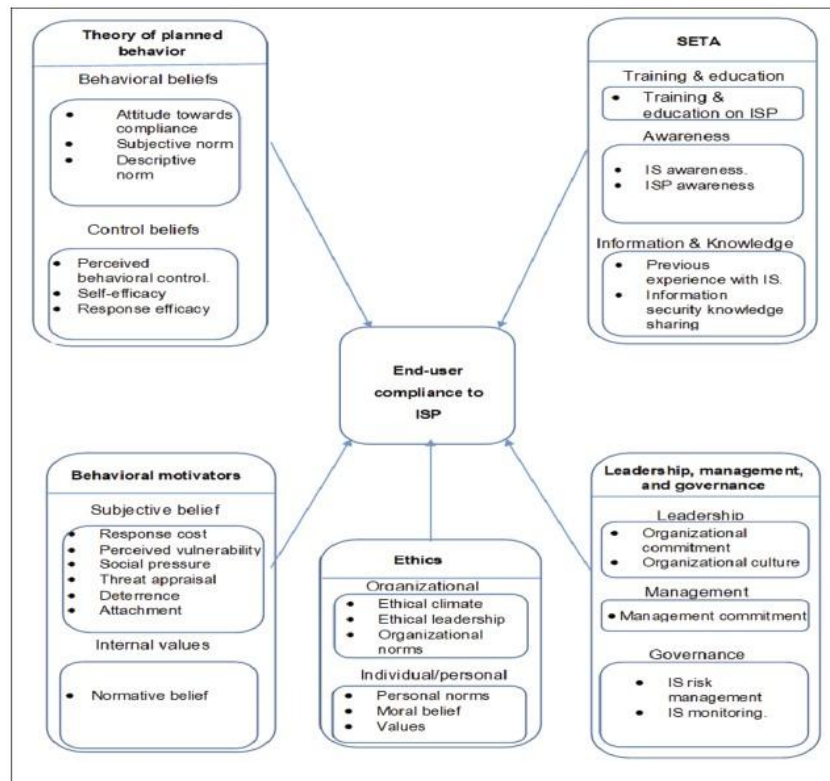


Fig. 1. End-User Compliance with Information Security Policy Framework (author developed)

This framework provides a comprehensive guide for enhancing end-user compliance to ISP specifically within South African government departments. By leveraging the identified factors and themes, government departments can systematically address the various elements that influence user behavior regarding information security. This framework offers actionable insights into how departments can implement and strengthen their security measures through targeted interventions based on the Theory of Planned Behavior, behavioral motivators, security education, training and awareness, (SETA), leadership, management and governance, and ethics. While most studies take a generic approach, this study incorporates the ethics-related factors, which are not commonly

addressed in most studies related to end-user compliance to ISP. Ethics is one of the factors that affect compliance with policies in the South African government [90, 91]. By including ethics, the framework acknowledges the moral and ethical considerations that influence end-user behavior, which is crucial in the context of public sector operations. The next phase of the study involves refining and validating the framework through qualitative research, including interviews with government employees and expert reviews. This will help assess the applicability and effectiveness of the framework in real-world settings. A limitation of this study is its reliance on literature review and theoretical constructs, which necessitates validation to ensure practical relevance.

5 Conclusion and Future Work

In this paper, the researchers conducted an investigation to identify the factors influencing end-user compliance with information security policies. The factors were used to develop a conceptual framework that can assist government departments in enhancing end-user compliance with information security policies. The main factors identified were the theory of planned behavior, behavioral motivators, security education, training and awareness, leadership, management and governance and ethics. This framework can be applied to government departments to enhance end-user compliance with information security policies. The limitation of this paper is that the conceptual framework has not been validated. Future research will be conducted through a qualitative research method to refine and validate the conceptual framework using government officials and an expert panel in a South African government department.

References

1. Mandal, D.: Towards an ontology for enterprise level information security policy analysis, pp. 492–499 (2021). <https://doi.org/10.5220/0010248004920499>
2. Wu, R., Ahn, G.-J., Hu, H.: Towards HIPAA-compliant healthcare systems. In: Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium - IHI 2012, p. 593 (2012). <https://doi.org/10.1145/2110363.2110429>
3. Alzahrani, L.: Factors impacting users' compliance with information security policies: an empirical study. *Int. J. Adv. Comput. Sci. Appl.* **12**, 437–447 (2021). <https://doi.org/10.14569/IJACSA.2021.0121049>
4. Beautelement, A., Sasse, M.A., Wonham, M.: The compliance budget: managing security behaviour in organisations, p. 134 (2008)
5. Ali, R.F., Dominic, P.D.D., Emad, S., Ali, A., Rehman, M.: Information security behavior and information security policy compliance: a systematic literature review for identifying the transformation process from noncompliance to compliance (2021)
6. Alotaibi, M., Furnell, S., Clarke, N.: Information security policies: a review of challenges and influencing factors (2014)
7. Liu, C., Wang, N., Liang, H.: Motivating information security policy compliance: the critical role of supervisor-subordinate Guanxi and organizational commitment. *Int. J. Inf. Manag.* **54**, 102152 (2020). <https://doi.org/10.1016/j.ijinfomgt.2020.102152>
8. Sohrabi Safa, N., Von Solms, R., Furnell, S.: Information security policy compliance model in organizations. *Comput. Secur.* **56**, 1–13 (2016). <https://doi.org/10.1016/j.cose.2015.10.006>

9. Aurigemma, S., Panko, R.: A composite framework for behavioral compliance with information security policies. In: Proceedings of the Annual Hawaii International Conference on System Sciences, pp. 3248–3257 (2012). <https://doi.org/10.1109/HICSS.2012.49>
10. Mani, D., Mubarak, S., Heravi, A., Choo, K.-K.R.: Employees' intended information security behaviour in real estate organisations: a protection motivation perspective. In: 2015 Americas Conference on Information Systems, AMCIS 2015, pp. 1–11 (2015)
11. Kirlappos, I., Parkin, S., Sasse, M.A.: "Shadow security" as a tool for the learning organization. *ACM SIGCAS Comput. Soc.* **45**, 29–37 (2015). <https://doi.org/10.1145/2738210.2738216>
12. Tsohou, A., Karyda, M., Kokolakis, S.: Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. *Comput. Secur.* **52**, 1–24 (2015). <https://doi.org/10.1016/j.cose.2015.04.006>
13. Ponemon Institute: 2022 Cost of Insider Threats Report Global Report (2022)
14. Cannoy, S.D., Salam, A.F.: A framework for health care information assurance policy and compliance. *Commun. ACM* **53**, 126 (2010). <https://doi.org/10.1145/1666420.1666453>
15. Arcy, J.D., Teh, P.: Predicting employee information security policy compliance on a daily basis: the interplay of security-related stress, emotions, and neutralization. *Inf. Manag.* **56**, 103151 (2019). <https://doi.org/10.1016/j.im.2019.02.006>
16. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Effects of individual and organization based beliefs and the moderating role of work experience on insiders' good security behaviors. In: Proceedings of the 12th IEEE International Conference on Computational Science and Engineering, CSE 2009, vol. 3, pp. 476–481 (2009). <https://doi.org/10.1109/CSE.2009.484>
17. Beris, O., Beautelement, A., Sasse, M.A.: Employee rule breakers, excuse makers and security champions: mapping the risk perceptions and emotions that drive security behaviors. In: Proceedings of the 2015 New Security Paradigms Workshop, pp. 73–84 (2015). <https://doi.org/10.1145/2841113.2841119>
18. Ng, B.Y., Kankanhalli, A., (Calvin) Xu, Y.: Studying users' computer security behavior: a health belief perspective. *Decis. Support Syst.* **46**, 815–825 (2009)
19. Yazdanmehr, A., Wang, J.: Employees' information security policy compliance: a norm activation perspective. *Decis. Support. Syst.* **92**, 36–46 (2016). <https://doi.org/10.1016/j.dss.2016.09.009>
20. Topa, I., Karyda, M.: Identifying factors that influence employees' security behavior for enhancing ISP compliance. In: Fischer-Hübner, S., Lambrinoudakis, C., López, J. (eds.) *Trust-Bus 2015*. LNCS, vol. 9264, pp. 169–179. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-22906-5_13
21. Shih, S.P., Liou, J.Y.: Investigate the effects of information security climate and psychological ownership on information security policy compliance. In: Proceedings of the Pacific Asia Conference on Information Systems, PACIS 2015 (2015)
22. Caryn, D.: Cyberattacks : South Africa, you've been hacked (2021). <https://www.dailymaverick.co.za/article/2021-11-06-cyberattacks-south-africa-youve-been-hacked>
23. Toyana, M.: Cyber bandits target South Africa: Department of Justic... (2021). <https://www.dailymaverick.co.za/article/2021-09-09-cyber-bandits-target-south-africa-department-of-justice-space-agency-hit-by-ransomware-attacks/>
24. Balozian, P., Leidner, D.: Review of IS security policy compliance. *ACM SIGMIS Database DATABASE Adv. Inf. Syst.* **48**, 11–43 (2017). <https://doi.org/10.1145/3130515.3130518>
25. Corpuz, M.S.: The enterprise information security policy as a strategic business policy within the corporate strategic plan. In: Proceedings of the 15th Multi-Conference on Systemics, Cybernetics and Informatics, WMSCI 2011: Volume III, Orlando, FL, USA, pp. 275–279. International Institute of Informatics and Systemics (IIIS) (2011)

26. Hina, S., Durai, D., Panneer, D., Benjamin, P.: Institutional governance and protection motivation: theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Comput. Secur.* **87**, 101594 (2019). <https://doi.org/10.1016/j.cose.2019.101594>
27. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quart.* **34**, 523–548 (2010)
28. Yazdanmehr, A., Jawad, M., Benbunan-Fich, R., Wang, J.: The role of ethical climates in employee information security policy violations. *Decis. Support. Syst.* **177**, 114086 (2024). <https://doi.org/10.1016/j.dss.2023.114086>
29. Jiang, R., Zhang, J.: The impact of work pressure and work completion justification on intentional nonmalicious information security policy violation intention. *Comput. Secur.* **130**, 103253 (2023). <https://doi.org/10.1016/j.cose.2023.103253>
30. Lowry, P.B., Moody, G.D.: Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Inf. Syst. J.* **25**, 433–463 (2015). <https://doi.org/10.1111/isj.12043>
31. Mahmoud, A.Y.: Information security policies and their relationship with the effectiveness of the management information systems of major Palestinian universities in the Gaza Strip. *Int. J. Inf. Sci. Manag. (IJISM)* **15**, 1–26 (2017)
32. Da Veiga, A.: The influence of information security policies on information security culture: illustrated through a case study, pp. 22–33 (2015)
33. Li, Y.J., Hoffman, E.: Designing an incentive mechanism for information security policy compliance: an experiment. *J. Econ. Behav. Organ.* **212**, 138–159 (2023). <https://doi.org/10.1016/j.jebo.2023.05.033>
34. Parsons, K., McCormac, A., Butavicius, M., Ferguson, L.: Human factors and information security: individual, culture and security environment. *Command Control Commun. Intell. Div.* **45** (2010). <https://doi.org/10.14722/ndss.2014.23268>
35. Son, J.: Information & management out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Inf. Manag.* **48**, 296–302 (2011). <https://doi.org/10.1016/j.im.2011.07.002>
36. Julisch, K.: Security compliance, p. 71 (2009). <https://doi.org/10.1145/1595676.1595687>
37. Bauer, S., Bernroider, E.W.N.: From information security awareness to reasoned compliant action. *ACM SIGMIS Database DATABASE Adv. Inf. Syst.* **48**, 44–68 (2017). <https://doi.org/10.1145/3130515.3130519>
38. Ali, R.F., Dominic, P.D.D.: Investigation of information security policy violations among oil and gas employees: a security-related stress and avoidance coping perspective. *J. Inf. Sci.* **50**, 254–272 (2024). <https://doi.org/10.1177/01655515221087680>
39. Alraja, M.N., Butt, U.J., Abbod, M.: Information security policies compliance in a global setting: an employee's perspective. *Comput. Secur.* **129**, 103208 (2023). <https://doi.org/10.1016/j.cose.2023.103208>
40. Ifinedo, P.: Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. *Comput. Secur.* **31**, 83–95 (2012). <https://doi.org/10.1016/j.cose.2011.10.007>
41. Cheng, L., Li, Y., Li, W., Holm, E., Zhai, Q.: Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory. *Comput. Secur.* **39**, 447–459 (2013). <https://doi.org/10.1016/j.cose.2013.09.009>
42. Wang, X., Wang, C., Sun, Z., Wang, C.: An optimal coupling incentive mechanism concerning insider's compliance behavior towards marine information security policy. *J. Ocean Eng. Sci.* **8**, 573–575 (2023). <https://doi.org/10.1016/j.joes.2022.05.023>

43. Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., Aleassa, H.: Information security policy compliance: an empirical study of ethical ideology. In: Proceedings of the Annual Hawaii International Conference on System Sciences, pp. 3018–3027 (2013). <https://doi.org/10.1109/HICSS.2013.272>
44. Khando, K., Gao, S., Islam, S.M., Salman, A.: Enhancing employees information security awareness in private and public organisations: a systematic literature review. *Comput. Secur.* **106**, 102267 (2021). <https://doi.org/10.1016/j.cose.2021.102267>
45. Faizi, S.M., Rahman, S.S.M.: Effect of fear on behavioral intention to comply. In: ACM International Conference Proceeding Series, pp. 65–70 (2020). <https://doi.org/10.1145/3404663.3404685>
46. PwC: The Global State of Survey 2018 Singapore highlights (2018)
47. PwC: The Global State of Survey 2020 (2020)
48. CISCO: Security Outcomes Report. 3 (2022)
49. Allassaf, M., Alkhalifah, A.: Exploring the influence of direct and indirect factors on information security policy compliance: a systematic literature review. *IEEE Access* **9**, 162687–162705 (2021). <https://doi.org/10.1109/ACCESS.2021.3132574>
50. Niekerk, J.F.V., Solms, R.V.: Information security culture: a management perspective. *Comput. Secur.* **29**, 476–486 (2010). <https://doi.org/10.1016/j.cose.2009.10.005>
51. Stewart, H., Jürjens, J.: Information security management and the human aspect in organizations. *Inf. Comput. Secur.* **25**, 494–534 (2017). <https://doi.org/10.1108/ICS-07-2016-0054>
52. Al-Omari, A., El-Gayar, O., Deokar, A.: Security policy compliance: user acceptance perspective. In: Proceedings of the Annual Hawaii International Conference on System Sciences, pp. 3317–3326 (2012). <https://doi.org/10.1109/HICSS.2012.516>
53. Kitchenham, B.: Procedures for performing systematic reviews. *UK Keele Univ.* **33**, 28 (2004). <https://doi.org/10.1.1.122.3308>
54. Colquhoun, H.L., et al.: Scoping reviews: time for clarity in definition, methods, and reporting. *J. Clin. Epidemiol.* **67**, 1291–1294 (2014). <https://doi.org/10.1016/j.jclinepi.2014.03.013>
55. Page, M.J., et al.: The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, 372 (2021). <https://doi.org/10.1136/bmj.n71>
56. Furlan, A.D., Pennick, V., Bombardier, C., Van Tulder, M.: 2009 Updated method guidelines for systematic reviews in the cochrane back review group. *Spine (Phila. Pa 1976)* **34**, 1929–1941 (2009). <https://doi.org/10.1097/BRS.0b013e3181b1c99f>
57. Bauer, S., Bernroider, E.W.N., Chudzikowski, K.: Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Comput. Secur.* **68**, 145–159 (2017). <https://doi.org/10.1016/j.cose.2017.04.009>
58. Mavetera, N., Moroke, N.D., Sebetlele, A.: An empirical study of staff compliance to information security policy in a South African municipality. *Corp. Ownersh. Control* **13**, 1375–1384 (2015)
59. Johnston, A.C., Warkentin, M., Siponen, M.: An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. *MIS Q.* **39**, 113–134 (2017). <https://doi.org/10.25300/misq/2015/39.1.06>
60. Karim, N.A., Kaur, J., Khalib, M.N.: Benefit vs cost: examining factors of intention to comply information security policy. In: 2021 IEEE International Conference on Computing, ICOCO 2021, pp. 291–296 (2021). <https://doi.org/10.1109/ICOCO53166.2021.9673542>
61. Milicevic, D., Goeken, M.: Social factors in policy compliance - evidence found in literature to assist the development of policies in information security management. In: Proceedings of the Annual Hawaii International Conference on System Sciences, pp. 4476–4484 (2013). <https://doi.org/10.1109/HICSS.2013.488>

62. Herath, T., Rao, H.R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. *Eur. J. Inf. Syst.* **18**, 106–125 (2009). <https://doi.org/10.1057/ejis.2009.6>
63. Sohrabi, N., Maple, C., Furnell, S., Ajmal, M.: Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Gener. Comput. Syst.* **97**, 587–597 (2019). <https://doi.org/10.1016/j.future.2019.03.024>
64. Somestad, T., Karlzén, H., Hallberg, J.: The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Inf. Comput. Secur.* **23**, 200–217 (2015). <https://doi.org/10.1108/ICS-04-2014-0025>
65. Foth, M.: Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence, p. 9344 (2017). <https://doi.org/10.1057/ejis.2015.9>
66. Siponen, M., Vance, A.: Neutralization: new insights into the problem of employee information systems security policy violations. *Nature* **34**, 487–502 (2010). <https://doi.org/10.1038/174197b0>
67. Nasir, A., Arshah, R.A., Ab Hamid, M.R.: Information security policy compliance behavior based on comprehensive dimensions of information security culture: a conceptual framework, pp. 56–60 (2017). <https://doi.org/10.1145/3077584.3077593>
68. Chen, X., Chen, L.: Chen, Chen Factors that influence employees' security policy compliance behavior DECISION SCIENCES INSTITUTE Factors that influence employees' security policy compliance behavior: an Awareness-Motivation-Capability (AMC) perspective (2016)
69. Padayachee, K.: Taxonomy of compliant information security behavior. *Comput. Secur.* **31**, 673–680 (2012). <https://doi.org/10.1016/j.cose.2012.04.004>
70. Li, L., He, W., Xu, L., Ash, I., Anwar, M., Yuan, X.: Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *Int. J. Inf. Manag.* **45**, 13–24 (2019). <https://doi.org/10.1016/j.ijinfomgt.2018.10.017>
71. Nasir, A., Arshah, R.A., Rashid, M., Hamid, A.: A dimension-based information security culture model and its relationship with employees' security behavior: a case study in Malaysian higher educational institutions. *Inf. Secur. J. A Glob. Perspect.* **28**, 55–80 (2019). <https://doi.org/10.1080/19393555.2019.1643956>
72. Chen, X., Chen, L., Wu, D., Perspective, A.: Factors that influence employees' security policy compliance: an awareness-motivation-capability perspective. *J. Comput. Inf. Syst.* **58**, 312–324 (2018). <https://doi.org/10.1080/08874417.2016.1258679>
73. Rajab, M., Eydgahi, A.: Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Comput. Secur.* **80**, 211–223 (2019). <https://doi.org/10.1016/j.cose.2018.09.016>
74. Palanisamy, R., Norman, A.A., Kiah, M.L.M.: Compliance with bring your own device security policies in organizations: a systematic literature review. *Comput. Secur.* **98**, 101998 (2020). <https://doi.org/10.1016/j.cose.2020.101998>
75. Chen, H., Li, W.: Understanding commitment and apathy in is security extra-role behavior from a person-organization fit perspective, 3001 (2019). <https://doi.org/10.1080/0144929X.2018.1539520>
76. Ali, R.F., Dominic, P.D.D., Ali, K.: Organizational governance, social bonds and information security policy compliance: a perspective towards oil and gas employees. *Sustainability* **12**, 1–27 (2020). <https://doi.org/10.3390/su12208576>
77. Siponen, M., Vance, A.: Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Q.* **34**, 487–502 (2010)
78. Choi, M., Song, J.: Social control through deterrence on the compliance with information security policy. *Soft. Comput.* **22**, 6765–6772 (2018). <https://doi.org/10.1007/s00500-018-3354-z>

79. Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J.: Variables influencing information security policy compliance: a systematic review of quantitative studies. *Inf. Manag. Comput. Secur.* **22**, 42–75 (2014). <https://doi.org/10.1108/IMCS-08-2012-0045>
80. Siponen, M., Pahlila, S., Mahmood, M.A.: Compliance with information security policies. *IEEE Comput. Soc.* **43**, 64–71 (2010)
81. Ifinedo, P.: Roles of organizational climate, social bonds, and perceptions of security threats on is security policy compliance intentions. *Inf. Resour. Manag. J.* **31**, 53–82 (2017). <https://doi.org/10.4018/irmj.2018010103>
82. Choi, Y.: Human resource management and security policy compliance. *Int. J. Hum. Cap. Inf. Technol. Prof.* **8**, 68–81 (2017). <https://doi.org/10.4018/ijhcitp.2017070105>
83. Alfawaz, S., Nelson, K., Mohannak, K.: Information security culture: a behaviour compliance conceptual framework BT. In: 8th Australasian Information Security Conference, AISC 2010, 19 January–20 January, 2010. *Conferences in Research and Practice in Information Technology Series*, vol. 105, pp. 47–55 (2010)
84. D’Arcy, J.D., Hovav, A., Galletta, D.: User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach (2009). <https://doi.org/10.1287/isre.1070.0160>
85. Sommestad, T., Karlzén, H., Hallberg, J.: The theory of planned behavior and information security policy compliance. *J. Comput. Inf. Syst.* **59**, 344–353 (2019). <https://doi.org/10.1080/08874417.2017.1368421>
86. Coertze, J.: A framework for information security governance in SMMEs (2012)
87. Fitzgerald, T.: Information security governance simplified from the boardroom to the keyboard (2019)
88. Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T., Kagaya, T.: Information security governance framework (2009). <https://doi.org/10.1145/1655168.1655170>
89. Wang, X., Xu, J.: Deterrence and leadership factors: Which are important for information security policy compliance in the hotel industry. *Tour. Manag.* **84**, 104282 (2021). <https://doi.org/10.1016/j.tourman.2021.104282>
90. Shava, E., Mazenda, A.: Ethics in South African public administration: a critical review (2021)
91. OECD.: Public Sector Integrity Management Framework. p. 33 (2005)



ECRIVENT
Professional Editor

CERTIFICATE OF EDITING

*Odelia Tait
Groot Brak
Mosselbay
Western Cape*

*Email: editor@mosaik.com
Phone: 083-982-7863*

February 2, 2026

CERTIFICATE OF EDITING

SAKHILE CHARITY DORIES LEKHULENI,

Student Number: 34906592
College: Computer Science
Degree: Master of Science
Institute: UNISA
Supervisor: Prof Adèle Da Veiga

This serves to confirm that copy-editing and proofreading services were rendered to *Sakhile Charity Dorries Lekhuleni, Student No:34906592 for the Master's degree "A FRAMEWORK FOR END-USER COMPLIANCE WITH THE INFORMATION SECURITY POLICY IN GOVERNMENT INSTITUTIONS"*

I am a member of the Professional Editors' Guild (member number TAI001) and commit to the following codes of practice (among others):

1. I have completed the work independently and did not sub-contract it out.
2. I kept to the agreed deadlines and/or communicated changes within a reasonable time frame.
3. I treated all work as confidential and maintained objectivity in editing.
4. I did not accept work that could be considered unlawful, dishonest or contrary to public interest.

I uphold the following editing standards:

1. Proofreading for mechanical errors such as spelling, punctuation, and grammar.
2. Copy-editing that includes the organisation and logical flow of content, basic formatting (headings, page numbers), and eliminating unnecessary repetition.
3. Checking citation style is correct, punctuating as needed and flagging incorrect references.
4. Editing was done for the dissertation, but not for the Appendices.

Other editing done specific to the dissertation:

- Passive voice changed to active voice.
- British English used in the dissertation.

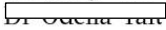
- Document corrected to the same format for all fonts and styles.
- Future tense changed to past tense or present tense.
- Decreased wordiness.
- Punctuation added and corrected.
- Only spelling errors were corrected for interview participant statements, not the grammar, as these are the participant's own words that are quoted.
- Corrected all spacing to 1.5.
- Reference checking as per the APA 7th edition.
- Consistency in dissertation.

I confirm that I have met the above editing standards and professional ethical practice. The content of the work edited remains that of the student.



[Handwritten signature]

Sincerely


Editor