



Faculty of Informatics and Design

Perception of employees concerning information security policy compliance: Case studies of a European and South African university

By

**STEVEN LUBUBU
(209002409)**

Thesis submitted in fulfilment of the requirements for the degree
Master of Technology: Information Technology

Supervisor: Dr Michael Twum-Darko

**CAPE TOWN
AUGUST 2018**

CPUT copyright information: The thesis may not be published either in part (in scholarly, scientific or technical journals), or as a whole (as a monograph), unless permission has been obtained from the University.

DECLARATION

I, **Steven Lububu**, declare that the contents of this thesis represent my own unaided work, and that the thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

Signed

Date

ABSTRACT

This study recognises that, regardless of information security policies, information about institutions continues to be leaked due to the lack of employee compliance. The problem is that information leakages have serious consequences for institutions, especially those that rely on information for its sustainability, functionality and competitiveness. As such, institutions ensure that information about their processes, activities and services are secured, which they do through enforcement and compliance of policies. The aim of this study is to explore the extent of non-compliance with information security policy in an institution.

The study followed an interpretive, qualitative case study approach to understand the meaningful characteristics of the actual situations of security breaches in institutions. Qualitative data was collected from two universities, using semi-structured interviews, with 17 participants. Two departments were selected: Human Resources and the Administrative office. These two departments were selected based on the following criteria: they both play key roles within an institution, they maintain and improve the university's policies, and both departments manage and keep confidential university information (Human Resources transects and keeps employees' information, whilst the Administrative office manages students' records).

This study used structuration theory as a lens to view and interpret the data. The qualitative content analysis was used to analyse documentation, such as brochures and information obtained from the websites of the case study's universities. The documentation was then further used to support the data from the interviews.

The findings revealed some factors that influence non-compliance with regards to information security policy, such as a lack of leadership skills, favouritism, fraud, corruption, insufficiency of infrastructure, lack of security education and miscommunication. In the context of this study, these factors have severe consequences on an institution, such as the loss of the institution's credibility or the institution's closure. Recommendations for further study are also made available.

Keywords: Information and Communication Technology (ICT) and information security, institutional services and information security, information management and information security, information leakage and Compliance Policy.

ACKNOWLEDGEMENTS

I thank God for His grace, favour and unconditional love towards me during this period. Without you Jesus, this study would not have been successfully completed.

I wish to thank:

- Dr Michael Twum-Darko, my main supervisor, for his wise academic advice and support;
- Dr André de la Harpe, for his attentive approachability and constant support; and
- Dr Pieter Wagenaar, the external supervisor from VU University Amsterdam, for his support and contribution.

Thank you, Jesus Christ, for being there for me.

DEDICATION

This thesis is dedicated to me “**Steven Lububu**” for my personal and self-encouragement, support and prayers.

TABLE OF CONTENTS

DECLARATIONi

ABSTRACT ii

ACKNOWLEDGEMENTS iii

DEDICATION..... iii

LIST OF FIGURESiv

LIST OF TABLESiv

GLOSSARY.....

CHAPTER ONE: INTRODUCTION..... 1

 1.1 INTRODUCTION..... 1

 1.2 RESEARCH BACKGROUND 1

 1.3 PROBLEM STATEMENT 2

 1.4 AIMS AND OBJECTIVES..... 2

 1.5 RESEARCH QUESTIONS 3

 1.6 OVERVIEW OF LITERATURE 3

 1.7 OVERVIEW OF THEORETICAL UNDERPINNING 4

 1.8 OVERVIEW OF THE RESEARCH APPROACH..... 4

 1.8.1 Research Philosophy4

 1.8.2 Methodology5

 1.8.3 Research Design.....6

 1.9 RESEARCH METHOD 6

 1.9.1 Interviews.....6

 1.9.2 Documentation8

 1.10 PARTICIPANT SAMPLING..... 8

 1.11 ANALYSING DATA..... 8

 1.12 OVERVIEW OF UNITS OF ANALYSIS 9

 1.13 OVER VIEW OF ETHICAL CONSIDERATIONS 9

 1.14 STUDY LIMITATIONS..... 9

1.15 OVERVIEW OF CONTRIBUTION OF THE RESEARCH.....	9
1.16 STRUCTURE OF REST OF THE THESIS	10
1.17 SUMMARY	10
CHAPTER TWO: LITERATURE REVIEW	12
2.1 INTRODUCTION.....	12
2.2 INFORMATION AND COMMUNICATION TECHNOLOGY AND INFORMATION SECURITY	12
2.3 INSTITUTIONAL SERVICES AND INFORMATION SECURITY	15
2.3.1 Awareness Service and Information Security	16
2.3.2 Training and Education Service and Information Security	17
2.4 INFORMATION MANAGEMENT AND INFORMATION SECURITY	18
2.5 INFORMATION LEAKAGE	19
2.5.1 Information Leakage through Partnerships with Outsourcing Activities.....	20
2.6 INFORMATION POLICY.....	20
2.7 SECURITY POLICY COMPLIANCE	21
2.8 UNDERPINNING THEORY OF THE RESEARCH.....	22
2.8.1 Application of Structuration Theory.....	23
2.8.2 Human Agents	24
2.8.3 Technology	25
2.8.4 Institutional Properties of an Organisation	25
2.8.5 Structuration Model in Practice.....	25
2.8.6 Structuration Theory: Duality of Technology	26
2.9 SUMMARY	26
CHAPTER THREE: RESEARCH APPROACH	28
3.1 INTRODUCTION	28
3.2 RESEARCH DESIGN	28
3.3 TECHNIQUES AND PROCEDURES.....	28
3.4 UNIT OF ANALYSIS.....	29

Sampling Technique	29
3.5 DATA COLLECTION	29
3.5.1 Interviews.....	29
3.5.2 Documentation.....	30
3.6 DATA ANALYSIS.....	30
3.6.1 Qualitative Content Analysis.....	30
3.6.2 Interpretive Analysis.....	31
3.7 DATA QUALITY ASSURANCE.....	32
3.7.1 Data Validity.....	32
3.7.2 Data Reliability and Conformability.....	33
3.8 ETHICAL CONSIDERATION.....	33
3.8.1 Ethics and Consent.....	33
3.8.2 Confidentiality	34
3.9 SUMMARY	34
CHAPTER FOUR: FINDINGS AND INTERPRETATION	35
4.1. INTRODUCTION.....	35
4.2. PROCESS OF ANALYSIS.....	35
4.2.1 Overview of the methodology.....	35
4.2.2 Overview of qualitative analysis	36
4.2.3 The Case and unit of analysis	38
4.2.4 Overview of sampling process	39
4.3 ANALYSIS AND INTERPRETATION.....	40
4.3.1 INTRODUCTION	40
4.3.2 Answers to the research question	41
4.3.3 Factors of Interpretive Schemes for Information Security Policies.....	48
4.3.4 Factors of Norms for a culture of compliance	50
4.3.5 Factors of Facilities for Information Systems & Technology	55
4.4 INSTITUTIONALISING INFORMATION SECURITY POLICIES	57

4.4.1 INTRODUCTION	57
4.4.2 Implementation as Interpretive Schemes	59
4.4.3 Information systems as Facilities	61
4.4.4 Information Security Policies as Norm.....	64
4.4.5 Conclusion	66
4.5 PROPOSED GENERAL FRAMEWORK.....	66
4.6 SUMMARY	67 ⁶⁸
CHAPTER FIVE: CONCLUSION AND RECOMMENDATION	69
5.1 INTRODUCTION	69
5.2 OVERVIEW OF THE RESEARCH.....	69
5.3 ENFORCEMENT OF INFORMATION SECURITY POLICIES	70
5.4 FACTORS OF NON-COMPLIANCE OF INFORMATION SECURITY POLICIES.....	71
5.5 FACTORS OF COMPLIANCE FOR INFORMATION SECURITY POLICIES	72
5.6 RESEARCH CONTRIBUTIONS	73
5.6.1 Methodological Contribution.....	73
5.6.2 Theoretical Contribution	73
5.6.3 Practical Contribution.....	74
5.7 RESEARCH LIMITATIONS	74
5.8 CONCLUSION AND RECOMMENDATION AND FUTURE RESEARCH	74
REFERENCES	76
Appendix A: Introductory Letter for Data Collection.....	86
Appendix B: Permission to Conduct Institutional Research –Vu Amsterdam.....	87
Appendix C: Official Invitation for Mr. Steven L. Lububu	88
Appendix D: Interview Schedule for Top Management.....	89
Appendix E: Interview Schedule for Staff Members	92
Appendix F: Transcription for Top Management	95
Appendix G: Transcription for Staff Members	100

LIST OF FIGURES

Figure 1.1: Problem conceptualisation.....	2
Figure 2.1: Extended enactment of technologies-in-practice mode.....	24
Figure 4.1: Proposed General Framework.....	67

LIST OF TABLES

Table 4.1: Summary of categories and themes.....	37
Table 4.2: Main and Sub-units of analysis.....	39
Table 4.3: Participants from Sub-units.....	40

GLOSSARY

CD	compact disc
CPUT	Cape Peninsula University of Technology
DoT	Duality of Technology
ERP	enterprise resource planning
HR	Human Resources
ICT	Information and Communication Technology
InfoSecPol	Information Security Policy
IT	Information Technology
IS	Information Security
NGO	Non-governmental organisation
NPO	Non-profit organisation
PLM	Product Lifecycle Management
SETA	Security, Education, Training and Awareness
SMT	Structuration Model of Technology
ST	Structuration Theory
VU	Vrije Universiteit Amsterdam

CHAPTER ONE: INTRODUCTION

1.1 INTRODUCTION

Cape Peninsula University of Technology (CPUT) is the biggest institution of technology in the Western Cape, and it is argued that CPUT is a continual victim of security breaches due to employees' non-compliance with information security policies. Therefore, there was a need to understand the reasons for non-compliance with information security policies in this institution. Vrije Universiteit Amsterdam (VU) was also chosen, as the researcher had an opportunity to go overseas as an exchange student. It was interesting to research and establish if the same crises of security breaches also existed in a European University.

This Chapter provides an introduction to this study, which is based on the perception of employees concerning information security policy compliance. This topic is broken down into the following units: Section 1.1 looks at the case studies of a European and South African university, followed by the research background in Section 1.2. The problem statement is provided in Section 1.3, aims and objectives are mentioned in Section 1.4, research questions discussed in Section 1.5 and a literature review in section 1.6. This leads to the theoretical underpinning in Section 1.7, the methodical considerations are laid out in Section 1.8, data collection is highlighted in Section 1.9 and the participant sampling in Section 1.10. The analysis of the collected data is described in Section 1.11, the unit of analysis in Section 1.12, ethical considerations in Section 1.13, the limitations of the study in Section 1.14, the contribution of the research in Section 1.15, the structure of the thesis in Section 1.16 and a summary in Section 1.17.

1.2 RESEARCH BACKGROUND

The value derived from information makes institutions more responsible and accountable for their actions. As institutions rely fully on information for their functions, sustainability and growth, they have to ensure that the information received and distributed is secured through the employees' compliance with relevant Information Security Policies (InfoSecPol). The leakage of information is a major problem in institutions, especially in this era of technological advancement. Information leakage has serious consequences for institutions, including loss of resources, poor performance and the inability to effectively manage the institution's activities, which can lead to job losses or the closing down of institutions. Drawing from the works of Ifinedo (2014) and Safa and Von Solms (2016), information leakage is generated by employees because of their lack of compliance with the InfoSecPol.

1.3 PROBLEM STATEMENT

Disregard and non-compliance of InfoSecPol by employees in institutions or organisations continues to be a threat to the functioning, growth and sustainability of many institutions. As information is considered to be the most valuable asset of institutions, many institutions are totally reliant on information to drive their competitiveness (see Figure 1.1). As such, institutions ensure that information about their processes, activities and services are secured, which is done through the enforcement and compliance of policies by employees.

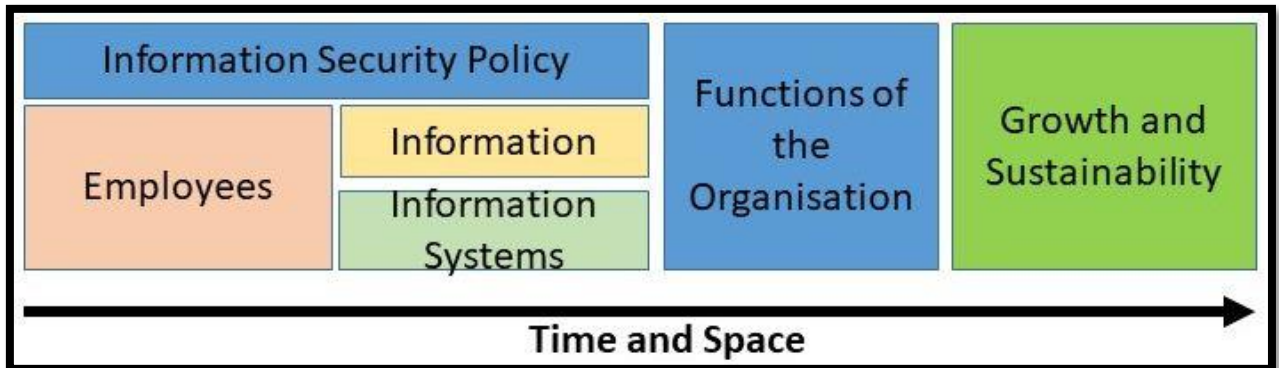


Figure 1:1 Problem Conceptualisation

The challenge with information leakages is the serious consequences for the institutions' ability to:

- i) sustain managerial goals and objectives;
- ii) carry out their service effectively and efficiently;
- iii) compete in the industry or market; and
- iv) manage the activities of the organisation.

1.4 AIMS AND OBJECTIVES

Therefore, the aim of this study is to explore the extent of non-compliance within an institution's InfoSecPol. Based on this aim, the main objective is to investigate the extent to which non-compliance of information security policies by employees in an institution would affect its functioning, growth and sustainability. The sub-objectives, therefore, were:

- i) To determine how information security policies are enforced in an institution;
- ii) To investigate the factors that influence non-compliance of the Information Security Policies in an institution; and
- iii) To determine the factors that influence compliance of the Information Security Policies in an institution.

1.5 RESEARCH QUESTIONS

Based on the problem statement and the objectives, the following research questions were articulated:

The main question is:

How can the non-compliance of InfoSecPol by employees in an institution be managed?

The sub-questions to address the main question are as follows:

- i) How are Information Security Policies enforced in an institution?
- ii) What are the factors that influence non-compliance of the Information Security Policies in an institution?
- iii) What are the factors that influence compliance of the Information Security Policies in an institution?

1.6 OVERVIEW OF LITERATURE

Information and Communication Technology (ICT) involves the use of various devices including computers, telephones and tablets. These devices enable communication and information to be sent, received, saved and changed. According to Madlock (2012), ICT has been adopted by large and small organisations by the way in which organisations communicate with clients, stakeholders, employees and vendors. Organisations or institutions share information through the use of ICT tools. Studies have recognised that sustainability issues need to be addressed in order to help organisations or institutions to succeed (Dao *et al.*, 2011). Thus, institutions rely on information for their sustainability, functionalities and competitiveness. As such, institutions need to protect information about their processes, activities and services, which they do through the enforcement and compliance of policies.

According to Bayrak (2012), technology has modified the way in which environments and work are being performed; this implies that information technology (IT) has an influence on society, which affects every aspect of human lives. Technology has improved the way institutions allocate and direct information to various areas (Bayrak, 2013), and these organisations or institutions need to implement security services such as education, training and awareness programmes in order to enforce policy compliance. These services educate and change employees' security behaviours, directly increasing employees' knowledge and compliancy. In many cases, these

security services help to safeguard information resources from abuse and leakages (Kolkowska *et al.*, 2017).

1.7 OVERVIEW OF THEORETICAL UNDERPINNING

In order to understand the reasons for non-compliance of the InfoSecPol in an institution, this study adopted a structuration theory (ST) and, in particular, the dimensions of Duality of Technology (DoT), as the theoretical lens through which to understand and interpret the interaction between technology, corporate information and employees:

- i) At the management level the problem was approached using the dimensions of DoT. In this study, the concepts of structural management were interpreted as a process that plans, organises, leads and controls the information within an entity. It also involved activities including the creation of policies, governance, security services, communication and compliance with InfoSecPols. The managers have the responsibility to educate, inform, motivate and support their employees through the learning process in order to enforce compliance with InfoSecPols; this was further supported by managers and other institutions' representatives; and
- ii) At the staff level, the problem was also approached using the dimensions of DoT. The study adopted concepts relating to IT infrastructure, preventive security systems, compliance checks, governance, policy, availability of resources and security services (such as awareness, education and training) that need to be accessed by employees in order to protect information. Furthermore, the concepts were extended due to the insights obtained from interviewees.

1.8 OVERVIEW OF THE RESEARCH APPROACH

The methodologies that were adopted to guide the data collection and analysis are discussed in-depth in Chapter 3. The following sub-sections are an overview of the methodological considerations used for this study.

1.8.1 Research Philosophy

research philosophy relates to knowledge improvement and the nature of that knowledge. The philosophy applied in this study contained key rules on how a person views the world; such views strengthened the research strategy and the methods chosen for the strategy (Du Plooy-Cilliers *et al.*, 2014). The paradigms in social science are referred to as world views and, therefore, when researchers are following a particular paradigm, they adopt a specific way of studying the phenomena which are relevant to their field (Fouché & Delpont, 2011). The research philosophy

for this study includes ontological and epistemological stances, as described in the following sub-sections.

1.8.1.1 Ontological Stance

Ontologically, the phenomenon was considered as subjective and given the nature as described in the problem statement. It sought to explore the embedded nature of knowledge and how human assumptions of the world are viewed, so as to understand the reality in which participants will reveal the scientific truth (Bhattacharjee, 2012). The question, therefore, was: "What is the reality in the problem and how can it be known?" As such, a subjectivist view is aligned with the interpretivist epistemology of knowing the reality; this subjectivism is used as a background to the interpretivist epistemology this study followed. Thus, the concern is to understand and interpret the problem, that is, the extent of non-compliance of the InfoSecPol in an institution as a social phenomenon and what reality can come out of its existence.

1.8.1.2 Epistemological Stance

Epistemologically, the study considered what counts as knowledge, what are the limitations thereof in the phenomenon and how the extracted nature of the knowledge will contribute to the existing body of knowledge. Therefore, the adopted stance required the selection of one of the three main components of epistemology: positivism, realism and interpretivism. Each of these components have a key difference that influences the way individuals think, concerning the research process, assumptions, concepts and research problems, which are considered important (Du Plooy-Cilliers *et al.*, 2014). This research study was applied and discussed through the interpretivist paradigm, as the research aim was to study reality subjectively in order to understand and explain the causes of employees' non-compliance of InfoSecPol in an institution.

1.8.2 Methodology

According to Neuman (2011), a research approach refers to a way of thinking about conducting a research study. It describes either explicitly - or implicitly - the purpose of the research, the role of the researcher(s), the stages of research and the method of data analysis. This study used an interpretive, qualitative case study as the research approach, which facilitated the exploration of phenomenon within its context using a variety of data sources. Therefore, the issue was explored through a variety of lenses, which allowed deferent perspectives of the phenomenon to be revealed and understood (Baxter & Jack, 2008; Fouché & Delport, 2011). This was the foundation for the choice of using CPUT and VU Amsterdam University (VU) for the case studies.

An interpretive qualitative case study was adopted in order to focus on actuality and relevance settings, such as an individual's life, institutional processes and international relations. Drawing from Yin (2013), the adoption of the interpretive qualitative case study was to produce new strategies and techniques on how to implement InfoSecPols. The focus was to understand the causes affecting a specific situation and to come up with a broad generalisation that depends on the evidence from the cases studied; thus, to propose a general framework to be used to manage InfoSecPol compliance in an institution.

1.8.3 Research Design

This case study followed an interpretive qualitative design approach, which is an extensive study with the objective being to investigate (in detail) an existing phenomenon for the following reasons:

- i) The causes of security breaches;
- ii) Factors that can enforce security; and
- iii) Factors that can motivate employees to comply with Information Security Policies in order to protect information within an institution.

The design approach led to an understanding of the meaningful characteristics of actual situations, such as an individual's life, and institutional and managerial processes. Furthermore, the approach offered the insight to achieve a broad generalisation that depended on empirical evidence from the cases that were studied (Babbie, 2013). CPUT was selected as a case study, based on the outcome of preliminary investigations on security breaches and leakages occurring every year. For example, CPUT students receive unofficial results from their colleagues or from other staff members, who are working in the departments. On the other hand, VU was selected because of the researcher's involvement in the student exchange programme, which offered the opportunity to determine if the same crises of security breaches occur at VU.

1.9 RESEARCH METHOD

Data was collected in the form of gathering various materials from identified sources towards achieving the objectives of studying the phenomena. Therefore, drawing from Bhattacharjee (2012), the data was collected from participants in the form of a scientific investigation using techniques such as interviews and documentation. The documentation method was used to support the interviews.

1.9.1 Interviews

There are three main types of interviews techniques:

- i) Structured interviews are a quantitative research method usually employed in survey study and is based on a fixed set of questions;
- ii) Unstructured interviews generate qualitative data by using open questions, which allows participants to talk in-depth by choosing their own words; and
- iii) Semi-structured interviews allow the participants to express their views, understanding and explanations of the phenomenon of the study.

The study used the semi-structured interview technique, which was considered most suitable, primarily for four reasons:

- i) The semi-structured interview allows the participants to express their views and answer the research questions in detail;
- ii) it allows instant probing of participants' responses;
- iii) it allows adjustment of the interview guide during the process; and
- iv) it does not allow for a specific number of interviewees, which could affect the richness of the data.

This helped to get clarification and to expand on views through further explanations, thereby making the data rich.

HR and Administrative office were the two departments selected. The reasons for selecting these two departments were based on the following criteria:

- i) these two departments play key roles within an institution;
- ii) they maintain and improve the university's policies;
- iii) HR transects and manages employees and students' information; and
- iv) the Administrative office keeps and processes students' information.

Therefore, it was necessary to understand the meaningful characteristics of the actual situations of security breaches happening within the institution. The participants were selected based on criteria such as positions, roles and responsibilities assumed within the departments (including HR managers, administrator managers, strategic managers, secretaries, assistant managers and other staff working within the selected departments).

The participants from HR were the most representative, who have key roles and positions in the universities. They maintain and improve the university's HR by planning, implementing and evaluating employees' relations and HR policies, services and practices.

The participants from the Administration office have key roles in providing administrative support and managing students' queries. They also manage students' data, and prepare and keep the students' and university records.

1.9.2 Documentation

The documentation discussed in this study consists of secondary sources of information that had been obtained and interpreted by other researchers. This is a set of information recorded in books, articles and other websites or publications. This study used available information from the selected universities (such as brochures and websites) to collect data about this research. The information obtained served as a support to the data collected from the interviews.

1.10 PARTICIPANT SAMPLING

The sampling was divided into probability and non-probability sampling (Neuman, 2011):

- i) Probability sampling is used when the study aims to generalise the findings numerically. It is usually associated with the quantitative methodology including survey and experimental strategies; and
- ii) Non-probability sampling is the process used in qualitative methods (Bhattacharjee, 2012). It is a non-numerical method, is non-random and can be subjected to a sampling bias by the researcher.

1.11 ANALYSING DATA

The data that was collected - using both the semi-structured and documentation techniques - was analysed. The data analysis process involved splitting data into small chunks that allow for sense making (Babbie & Mouton, 2011). The analyses were done separately though the findings were combined.

The interpretive approach was followed in the analysis of the data that was collected during the interviews. The data was analysed and described separately for each participant based on his or her experiences, views and perspectives on the phenomenon:

- i) This study used ST as a lens to view and interpret the data, which was based on the objectives of this research study, and which guided the data analysis process;
- ii) This study used qualitative content analysis to analyse the documentation (such as brochures and information obtained from the websites) of the university case studies. The documentation was used to support the data from the interviews; and

- iii) Additionally, this study followed an interpretive analysis design approach to analyse the words of the participants from interviews.

1.12 OVERVIEW OF UNITS OF ANALYSIS

The unit of analysis is the foundation of each case (Ponelis, 2015). According to Bhattacharjee (2012), the unit of analysis can be an individual such as a person, who has an experience that is of interest to the research. It may be an event, a social process or an organisation. For this study, the unit of analyses are the institutions identified, who use information (students' data) as part of their strategic business purposes. CPUT and VU who were used as the main units. Within the main units, HR and the Administration office were used as sub-units in the analysis of the data.

1.13 OVER VIEW OF ETHICAL CONSIDERATIONS

According to Babbie (2013), ethical considerations in research are recommended to ensure confidentiality and anonymity of participants during the research period. To this effect, an ethical clearance letter was obtained from CPUT's ethics review committee and permission was provided from both universities for data collection. Thereafter, an informed consent letter requesting individual permission to collect data was sent to the participants. The consent letter informed the participants of the research objectives, their optional participation and that the collected data will be confidential. Furthermore, the consent letter clarified that the participants can choose to withdraw voluntarily at any time during the session without giving any reasons. The information obtained from the participants was kept anonymous and confidential.

1.14 STUDY LIMITATIONS

A qualitative and exploratory approach was followed in this study with a multiple-case study strategy to propose a general framework, which could be used to manage the InfoSecPol compliance in an institution. The study only collected data from CPUT in Cape Town and VU in the Netherlands. The participants considered in this study were employees from the selected institutions.

1.15 OVERVIEW OF CONTRIBUTION OF THE RESEARCH

The significance of this research is to add to the body of knowledge in terms of gaining understanding and new insights into the process of managing InfoSecPol compliance. The contribution of this study was to extend and support existing theories. The study was conducted to propose a general framework, which could be used to manage InfoSecPol compliance in an institution.

1.16 STRUCTURE OF REST OF THE THESIS

Chapter One is the introduction to the research and includes the background to the research problem. This is followed by a problem statement, research questions, aims and objectives of the research, contribution of the research, research limitation and ethical considerations of the study.

Chapter Two provides an in-depth literature review, which includes past scientific research by known scholars and authorities in InfoSecPol and the various phenomena that have been investigated. The Chapter ends with explanations of the proposed theory on Information Security (IS), which uses ST as a lens to view and interpret the data.

Chapter Three covers the research approaches and methodologies. It provides an overview of the philosophical assumptions, paradigms and research approach. It also describes the data collection methods and analysis strategies used. The validation and ethical considerations are then discussed.

Chapter Four presents the theory used as a lens to view and interpret the data. The Chapter also presents the analytical process that was followed to analyse the data from the interviews and provides answers to the research questions.

Chapter Five discusses the research objectives, contribution, limitations, recommendation and future research studies. Finally, the Chapter concludes the research study.

1.17 SUMMARY

This Chapter introduced the research background and the aim of this study, which is to explore the extent of non-compliance with the InfoSecPol in an institution. Research questions were designed to provide guidelines to investigate the phenomenon being studied. An overview of the literature was discussed as well. After that, the Chapter discussed the research philosophy as knowledge improvement and the nature of that knowledge, which includes ontological and epistemological stances. Ontologically, the phenomenon is considered as subjective; it explores the embedded nature of knowledge and how human assumptions of the world were viewed to understand the reality. Thus, the concern is to understand and interpret the problem: the extent of non-compliance of the InfoSecPol in an institution as a social phenomenon and what reality can come out of its existence. Epistemologically, the study considered what counts as knowledge, what the limitations are in the phenomenon and how the extracted nature of the knowledge will

contribute to the existing body of knowledge. Furthermore, this study describes, explicitly and implicitly, the purpose of the research, the role of the researcher(s), the stages of research and the method of data analysis.

The study followed the interpretive qualitative design approach, which facilitated the exploration of the phenomenon within its context using a variety of data sources. Data was collected from both CPUT and VU in the form of gathering various materials from the identified sources, towards achieving the objectives of studying the phenomena. The study used the semi-structured interview technique, which was considered most suitable, primarily as it allows the participants to express their views and answer the research questions in detail.

Finally, the Chapter discussed the overview of the ethical considerations to ensure confidentiality and anonymity of the participants. The next Chapter discusses the literature review of this study.

CHAPTER TWO: LITERATURE REVIEW

2.1 INTRODUCTION

The previous Chapter provided an introduction to this study, which is based on the perception of employees on the Information Security Policies and the non-compliance by employees in an institution. To do so, a case study of a European and a South African university was undertaken. The previous Chapter also discussed how to determine the extent of non-compliance of InfoSecPol in an institution. The research questions were discussed and they provided guidelines to investigate the phenomenon being studied. This Chapter presents a review of the relevant literature in order to understand what work has been done - and is being done - to address similar phenomena. The focus areas include Information and Communication Technology (ICT) in Section 2.2, institutional services in Section 2.3, information management in Section 2.4, information security in Section 2.5, information leakage in Section 2.6, information policy in Section 2.7, policy compliance in Section 2.8 and theories supporting the study in Section 2.9.

2.2 INFORMATION AND COMMUNICATION TECHNOLOGY AND INFORMATION SECURITY

ICT is the combination of all devices, networking components, applications and systems that allow people and organisations to communicate in the digital world. According to Luo and Bu (2016), ICT is a combination of telecommunications such as telephone lines and wireless, computers including enterprise software and storage, and audio-visual equipment. Nyaanga (2012) asserted that ICT has a revolutionary impact on social transformation, as well as economic and political systems. For example, social networking media such as Facebook or Twitter are used without barriers between the sender and receiver.

On the other hand, IS can be understood as the state of protection against the illegal use of information, specifically concerning electronic data and the strategies taken in order to achieve this protection (Hostland *et al.*, 2010). According to Shih *et al.* (2016), IS, in its nature, starts with a basic understanding of risk and how to manage those risks. In some way, IS makes employees aware of the organisational structure and security threats, and gives employees an understanding of how to identify the risks and secure information (Soomro *et al.*, 2016). Organisations need a continual IS awareness in order to minimise the risk of information leakage and enforce InfoSecPol compliance (Siponen *et al.*, 2014).

Concerning the use of information security in organisations, a consideration is needed to be given to the combination of the human aspect and technology. According to Da Veiga and Martins

(2015), technology itself cannot work or provide security of information resources. There is a need for the integration between people and technology through providing learning, education and awareness processes. People need a certain awareness - and training - based on security issues in order to protect information (Ifinedo, 2014). The learning process will give suitable knowledge on how to use information resources and to avoid security leakages (Elhai & Hall, 2016). Organisations need IS because it is central to understanding the risks and how to manage them, as it forms part of organisational objectives. IS instructs, educates and gives an understanding on how to control risks with regards to information (Safa *et al.*, 2015).

From a societal and economic point of view, ICT has changed how people work, communicate, do business, learn and live. It has provided vast changes in society as people are moving from face-to-face communication to the digital space, which involves online chatting, transaction and instant messages. According to Nord *et al.* (2017), ICT enables learning process, transactions, connections with the market leaders in global competition and opportunities for incorporating both technology and operations in everyday processes. It provides global connections, communication and empowerment. The presence of ICT in society has generated an information explosion era, which enables organisations to wisely manage knowledge and information databases, make managerial decisions and improve its competitiveness. While IS informs and clarifies to the user the particular aims and objectives of IS management, IS is also connected to the organisations' strategies and goals in terms of education, instruction and understanding of the risks in society or institutions (Hostland *et al.*, 2010).

ICT has a positive impact on an organisation's competitiveness and performance which, according to Kayombo and Mlyakado (2015), is determined by the alignment between the organisation's ICT and its particular needs and ability for ICT to enable information sharing and integration. On this basis, Chisita and Chinyemba (2017) argued that a country's development and the organisations' quality control and globalisation determine the extent to which ICT can contribute to competitiveness. ICT is an important resource for competitiveness on both country and organisational level. This means that the organisation has to view ICT as an important asset, which connects international resources, partners and external stakeholders to pay off for their competitive disadvantage and resource controls. For example, Yunis *et al.* (2017) said that ICT enabled organisational structure and coordination mechanisms to facilitate operative information sharing and knowledge integration across organisations. Thus, the information can be shared inside and outside, as well as formally and informally.

ICT is applied in an organisation as a mechanism of coordination that allows the control process of rules, routines, group problem solving and common knowledge. According to Kessy *et al.* (2006), ICT can facilitate information integration as information is viewed as the central task of organisations. IS can be used as a security education process that makes people aware of the institution's structure, security threats, and knowledge needed on how to control the risk in order to protect information (Keamey & Kruger, 2016).

The usability and coordination mechanism of ICT facilitates information integration by enabling the implementation and update of rules, which refer to the criteria that regulate the integration of information. An identical ICT system can ensure the application of these rules and their update if the rules change. In this way, the rule is enforced and the quality and value of integrated information is guaranteed. ICT serves as a medium for the organisation's routine, which generates information. For example, an enterprise resource planning (ERP) system is built on innovative ICT: it collects data and information from different business activities including manufacturing, marketing, sales and shopping and also provides and shares information across different departments. Thus, ERP systems are considered an organisational routine that improves the level of management and decision making. Additionally, ICT makes group problem solving and decision making less costly; by facilitating group coordination, ICT allows cost effective interactions between group members, through (*inter alia*) remote video conferencing in the Web 2.0 environment. Communication can be managed among members who are not known but who share common interests. Unfortunately, ICT faced several adoption challenges and generated problems and challenges to organisations and people.

In terms of the adoption of ICT, several organisations are not able to purchase its facilities due to the expensive costs, which are related to the purchase of infrastructure such as hardware and software, and includes their maintenance. Kessy *et al.* (2006) agree, stating that the implementation of ICT by organisations is affected by the cost of facilities. Also, Kayombo and Mlyakado (2015) found that some organisations lack the proper infrastructure that can accommodate ICT, particularly in developing countries. For example, some schools in rural areas of developing countries do not have electricity or the Internet and thus cannot operate computers. In the same context, Muljono (2017) found that ignorance and low literacy levels is a challenge to the adoption of ICT in educational and organisational systems. Some organisations lack the financial support to train or educate their employees on how to incorporate ICT into the working environment and be compliant with the policy on IS (Ifinedo, 2014).

In terms of issues and challenges generated by ICT, the advancement of ICT has produced an increase in cybercrime e.g. fraud, theft and corruption. Cybercriminals are using technology as a medium to leak information from targeted organisations. The development of digital data and the growing use of the Internet have together led to a higher level of crime, where cybercriminals gain illegal access to systems for the purpose of stealing money, private or organisational information. Drawing from this, Muljono (2017) revealed some of the challenges faced by organisations in terms of ICT adoption, which included the loss of control over the information accessed or distributed online, privacy of information, identity theft and information leakages. These challenges have serious consequences for organisations and people, particularly those who rely on the value of information to carry out their services effectively and efficiently, to compete in the market, to sustain organisational goals and objectives, and to manage the activities of the organisation. In some cases, the ICT issues led to loss of information, job losses or an organisation's closure.

2.3 INSTITUTIONAL SERVICES AND INFORMATION SECURITY

A service can be a valuable action, accomplishment or it an effort performed to satisfy a need or to achieve a demand. Sometimes, organisations provide services to their clients and partners for different reasons, which are either profit-oriented or non-profit based (Yildirim, 2016). For example, profit-oriented services include those provided by both private and public organisations and agencies. Non-governmental organisations (NGOs) and non-profit organisations (NPOs) do not provide services for the sake of profit; some of the services include education, awareness, eLearning and training. Organisations need these services in order to support employees by allowing set up and maintenance of users, knowledge and sharing agreements. According to Ifinedo (2014), institutional services run policies for improving services. Institutional services develop a communication sharing model among employees, increasing knowledge and establishing organisational service tools that identify and address service barriers.

On the other hand, Information Security is a security service that provides awareness of security issues. This security service is provided to employees and other users in order to protect information. As such, information security instructs, educates, and informs users and employees about security threats and how to manage the risks (Yunos *et al.*, 2016). Also, it is a strategy taken to understand threats and to avoid them (Bulgurcu *et al.*, 2010).

Concerning the use of institutional services, it depends on how the policies are implemented from one institution to another, as different institutions employ various approaches in the implementation of their IS policies. According to Boss *et al.* (2015), IS increases employees'

performance, knowledge, skills, protection and compliance. The increase of knowledge is due to many factors, including awareness of security policies, training and education, leadership skills and the support and motivation from management and government. These security approaches enable employees' awareness of security, provides new strategies and skills on how to avoid information leakage and protect data from unauthorised access. These services are designed to support employees by allowing the set up and maintenance of users, services achievements and sharing agreements through compliance.

Services that some institutions provide to their clients are derailed due to factors such as security breaches. According to Yu and Yang (2017), security breaches are caused when the organisational value relies on services that are provided and created intentionally or unintentionally by employees. Yu and Yang (2017) posited that security breaches lead to violations of privacy, abuse of customer or organisational rights, data insecurity and financial fraud.

This study has adopted awareness, training and education as top security services to provide an understanding of what it takes to protect against today's security challenges, to increase employees' knowledge on how to protect information against today's threats and to address compliance, to help employees better understand the policies, procedures and reporting. In this research, the objective was to determine how InfoSecPol are enforced, to investigate the factors that influence non-compliance with InfoSecPol, and to determine the factors that influence compliance with InfoSecPol in an institution. These objectives will be used to develop a descriptive framework.

The following sections present the theoretical foundations for these security services.

2.3.1 Awareness Service and Information Security

Awareness is the knowledge and understanding around something (such as security issues) and making people aware of the safekeeping of information assets (Furnell *et al.*, 2016). According to Yildirim (2016), security awareness is used particularly as an educational tool for members or employees that have direct or practical applications to the workplace and beyond. In addition, Siponen *et al.* (2014) said that "awareness service" includes an awareness of risks, danger, safety and valued resources, which is translated into action or behaviour that addresses those risks. Awareness service is part of IS because it involves knowledge and understanding about security threats. On this basis, Safa *et al.* (2015) discussed that IS increased knowledge through the learning and informing of security issues.

From awareness perspectives, Siponen *et al.* (2014) said that awareness is an educative service that gives ideas on how to deal with security threats. According to Parsons *et al.* (2014), security awareness educates and motivates employees for efficient IS and identifies risk of security leakages within organisations. For example, hackers upload fake anti-virus packages on their fake websites and request people to download their free anti-virus software. Unaware, people download the fake anti-virus and consequently end up with their devices infected with malware (malicious software) and their private information is stolen.

Other examples of employees' mistakes concerning IS behaviour include social engineering and phishing. Unaware employees are opening unknown attached files and emails, which is exposing them to any kind of cyberattack. Employees need assistance in order to change their security behaviour (Parsons *et al.*, 2014). Therefore, an awareness service is required in such situations so as to educate and instruct employees about security threats on the Internet, to avoid and prevent the risks so as to be competitive in the market. Such services enable efficiency of IS and can motivate employees to comply with the objectives of their organisations. IS plays an important role within various security services in terms of protection of knowledge, and provides an understanding of how to identify the risks and secure the information (Elhai & Hall, 2016).

However, this view is opposed by Choi and Lee (2015), who said that security awareness always has issues because it educates users in the form of general learning and does not give full and inclusive knowledge on InfoSecPol. As such, lack of inclusive knowledge and policy updates can generate information leakage. Furthermore, Shih *et al.* (2016) argued that organisations do not provide awareness services to their employees in order to avoid intentional and unintentional information leakage. Therefore, the lack of awareness services exposes organisations to endless security incidents.

2.3.2 Training and Education Service and Information Security

According to Karjalainen and Siponen (2011), different approaches have been proposed for training services such as psychological training approaches, theories- and process-based learning, security awareness approaches, situational approaches, social engineering preventive approaches and computer-based training. Furthermore, Xu *et al.* (2016) stated that these approaches educate, provide skills and inform the user on how to avoid information leakage, either intentionally or unintentionally. The training and education services form part of IS, which are provided to employees as security services and strategies used to identify risks. In addition, these

services provide technical skills and educative knowledge about IS (Ifinedo, 2014). IS influences the knowledge gap in terms of skills and understanding about security threats, and it aims to improve the knowledge gap, performance and security behaviour through the learning process (Xu *et al.*, 2016).

With regards to training, organisations adopt IS training as a common approach to improve employees' security behaviours and to ensure their compliance with InfoSecPols (Karjalainen & Siponen, 2011). According to Xu *et al.* (2016), organisations provide services to their clients and partners for either profit-oriented or non-profit reasons. As such, education and training services can be provided in different ways, such as traditional lectures, hands-on exercises, online training and emails based on security issues and updates.

Supporting the above authors, Yildirim (2016) added that, in order to improve the effectiveness of training services, organisations have to implement systems training related to the study of several behavioural theories. Other studies have shown that learning style is an important predictor of a subject's learning performance; this can be both by itself and through its collaboration with training techniques (Xu *et al.*, 2016; Ifinedo, 2014). Some training systems take into consideration the user's learning styles, and most aim to improve the learners' knowledge gap concerning information, security behaviour weaknesses, risk awareness and system security (Tsohou *et al.*, 2015). These are the key issues among organisations, for different reasons, which includes finance, availability, timing and negligence (Vance *et al.*, 2013). The knowledge gap and risk plan are important variables that influence security behaviour. On the other hand, Yunos *et al.* (2016) found that a training service is always unfinished and does not cover all users' learning styles. What's more, Kayombo and Mlyakado (2015) found that some organisations lack the financial support to train their employees; thus, the lack of training may cause information leakage as employees do not have the knowledge of how to avoid intentional and unintentional leakage.

2.4 INFORMATION MANAGEMENT AND INFORMATION SECURITY

Information management is about the cycle of organisational activity, the acquisition of information from different sources, the distribution of that information to people who are in need and its availability (Soto-Acosta *et al.*, 2016). According to Da Veiga and Martins (2015), information and IS are the foundation for an organisational lifecycle. Furthermore, Soto-Acosta *et al.* (2016) argued that the process of managing the entire lifecycle from the production through to the distribution can be referred to as product lifecycle management (PLM), which is a type of approach that

manages information - together with the product lifecycle - by enabling organisations to reduce product time-to-market, to be competitive as well as to produce a quality product.

According to Hostland *et al.* (2010), the objective of IS is to inform and clarify IS management; this is based on the operational techniques and goals within an organisation. Furthermore, Siponen *et al.* (2014) discussed that IS makes employees aware of security threats and focuses on the understanding of the risks and how to control them. In addition, organisations need information management in order to facilitate organisational lifecycle activity processes (Soto-Acosta *et al.*, 2015). Drawing from this, Saridakis *et al.* (2016) asserted that information management facilitates a collaborative platform with real-time control that can improve information access, distribution, exchange of knowledge, communication and accessibility of information.

The use of information management in an organisation benefits organisational lifecycle activity. It manages the information during lifecycle activities including production, information sharing, control and improved communication related to information (Soto-Acosta *et al.*, 2015). Similarly, Loenen (2015) found that information management is at the centre of organisational activities, as it coordinates and controls the organisational processes, and improves knowledge between employees.

The variations in the global economy are challenges to organisations. According to Vezzetti *et al.* (2014), some organisations have limited financial resources that can create a lack of connectivity with other organisations in terms of the product lifecycle process, and the purchasing of the necessary hardware and software. Likewise, Hostland *et al.* (2010) found that the internal and external transactions of information are exposed to various attacks related to the development of IT. Therefore, there is a need for an appropriate measure of information security to avoid security breaches.

2.5 INFORMATION LEAKAGE

Information leakage is a set of data that is leaked intentionally - or unintentionally - to an unauthorised party. The information leakage is applied to information or data considered confidential, which is not properly secured and can carry different levels of risks, including the inability to manage organisational operations (Chen & Ozer, 2017).

According to Desourdis *et al.* (2016), intentional leakage is for explicit purposes (such as monetary gain or sabotage), whereas unintentional leakage is generated by mistake. Drawing

from this, Tang and Zhang (2016) maintained that leakage can cause organisations to lose their competitive advantage in their respective fields. Information leakage may be caused by different reasons, including a lack of awareness, lack of specific skills in handling information or the inability to identify the causes of the occurring problem (Safa & Von Solms, 2016).

2.5.1 Information Leakage through Partnerships with Outsourcing Activities

Information leakage of an organisation's valuable assets to outsiders can be caused by outsourcing activities. According to Susanne et al. (2015), outsourcing providers can sell the information developed in their organisations to competitors, which can affect the competitiveness of the company. Furthermore, Kearney and (2016) discussed that the threatened organisation could lose their skills and competitive advantage in the marketplace, due to the risky behaviour of their partners.

2.6 INFORMATION POLICY

Information Policy refers to a set of rules and guidelines established by organisations to address particular security issues and to clarify the need for IS and its concepts. According to Bulgurcu *et al.* (2010), Information Policy is part of the integral organisation's objectives. It acts as a platform that protects information from illegal access. Other researchers have described Information Policy as a set of documentation that contains different instructions on IS. Furthermore, Yildirim (2016) maintained that Information Policy is a set of documentation aligning enterprise wide decisions on how to handle and protect information. According to Ifinedo (2014) and Crossler *et al.* (2013), Information Policy is established in order to avoid security breaches and secure information through compliance.

Information Policy is needed in organisations for the safety of both private and organisational aspects. Moreover, Boss et al. (2015) outlined that Information Policy increases employees' performance, knowledge, skills, protection and compliance. According to Boss *et al.* (2015), the increase of knowledge is due to many factors, including awareness of security policies, training and education, focus on leadership skills and the support and motivation from management and government.

With regard to the application of Information Policy in organisations, the policy must be clear, well defined, understandable and create a positive attitude of the organisation towards compliance. On this basis, Safa et al. (2016) stated that the policy must announce that information is the property of the organisation and must be protected from internal and external unauthorised access.

Similarly, Siponen et al. (2014) posited that employees need to be provided with information security education, awareness and training in order to be able to comply with the Information Policy. These factors enable employees' performance and provide new strategies and skills on how to avoid security breaches (Sommestad et al. 2014).

The key threats and challenges to Information Policy originate from employees who do not comply. According to Siponen et al. (2014), non-compliance with Information Policy has serious consequences for organisations, especially in terms of security breaches. In the same vein, Ifinedo (2014) discussed that organisations are exposed to security breaches generated by their employees due to non-compliance with the established Information Policy. Similarly, Sommestad et al. (2014) found that security breaches in organisations are caused by poor leadership skills, lack of awareness of policy, lack of training and lack of communication about the Information Policy between the management and employees.

Researchers have revealed that some of the consequences of non-compliance of Information Policy include the inability to sustain organisational goals and objectives, to carry out their service effectively and efficiently, to compete in the industry or market, and to manage the activities of the organisation (Ifinedo, 2014; Safa et al., 2016; Siponem et al., 2014; Sommestad et al., 2014). These consequences sometimes lead to job losses or an organisation's closure.

2.7 SECURITY POLICY COMPLIANCE

The term Policy Compliance refers to an implemented set of rules and regulations based on IS, where compliance is either in a state of being in accord with the implemented rules, guidelines and legislations or in the process of becoming so. Organisations establish policies in order to ensure the security of information resources; hence, employees have to follow and obey the security policy (Herath & Rao, 2009). In this regard, Bulgurcu et al. (2010) found that employees who comply with the IS rules and regulations of their organisations, enforce IS and protect information.

According to Ifinedo (2012), Information Policy is a set of documents that outline particular rules that must be complied with, for the protection of information from intentional - and unintentional - leakage. Furthermore, Kolkowska et al. (2017) stated that organisations have recognised that their employees are the weak link in IS; thus, the application of Policy Compliance for regulating employees' IS behaviours is important.

Organisations need Policies for regulating employees' IS behaviours and safeguarding informational resources from abuse and leakage. According to Kolkowska *et al.* (2017), the unique technique of management control is the implementation of policy on IS for regulating employees' IS behaviours. Previous researchers discussed that intentional - and unintentional - breaches are caused by employees who violate the InfoSecPol (Siponen *et al.*, 2014; Crossler *et al.*, 2013). Similarly, Chen and Li (2014) discussed that non-compliance with a policy is when employees fail to obey or to act according to the InfoSecPol. Therefore, implementing the InfoSecPol compliance and informing employees about it is important for the protection of information (Crossler *et al.*, 2013; Kolkowska *et al.* 2017; Siponen *et al.*, 2014).

Concerning the use of Policy Compliance in organisations: various studies have emerged explaining the importance of employees' compliance with the policy as a useful technique which influences the behaviours of their employees on protecting information (Bulgurcu *et al.*, 2010; Siponen & Willison, 2010). According to Siponen *et al.* (2010), various factors such as awareness of policy, communication about the policy and good management skills are employed to enforce Policy Compliance. Therefore, IS managers have to design and communicate with their employees the policy rules and regulations (Hedström *et al.*, 2013). According to Herath and Rao (2009), informing employees about the policy can allow them to put the policy into practice through compliance, which is in line with organisational learning processes and supports (Ifinedo, 2014). Therefore, Policy Compliance is used in organisations to safeguard information from misuse, abuse and information leakage.

Employees' non-compliance with InfoSecPol is a challenge for many organisations. According to Chen and Li (2014), employees' lack of compliance and lack of management skills are the causes of information leakage in organisations. Employees are the key problem with regards to IS breaches; this based on different reasons such as unawareness, lack of communication, carelessness, lack of incentives and the availability of resources. Drawing from the work of Stahl *et al.* (2012), employees' security behaviours are derailed by poor management skills through a poorly designed InfoSecPol.

2.8 UNDERPINNING THEORY OF THE RESEARCH

The application of theory in this study is to have a lens through which the phenomenon being studied and, in particular, the interplay between the various actors forming the phenomenon can be presented and explained (Zikmund *et al.*, 2010). As already alluded to in Chapter 1, this research study used structuration theory (ST) as a lens through which the phenomenon was

viewed and interpreted - particularly as a social theory - which can be used to study socially constructed phenomenon with embedded socio-technology processes. ST was found to be appropriate for this study because of the phenomenon's embedded interplay between employees' behaviour and attitude and appropriate use of technology and IS. In other words, the ST guided the design of the data collection instrument and the analysis of the collected data. The dimension of DoT within the ST (Orlikowski, 2000) was deployed to understand the interaction between technology, people and processes in an institution. The understanding of this interaction provided insights into the limits and chances of human decision, technology innovation, and the organisational design and use of elements such as rules, policy, control mechanisms and communication.

2.8.1 Application of Structuration Theory

ST was used as a lens through which to understand and interpret the interaction of employees and the structural features of an institution. Thus, the study considered employees as human actors who take actions by using technology facilities. The structure is the outcome of human actions, (Orlikowski, 2000) posits that:

- Duality of Technology refers to the technology that has been created, modified and used by the human throughout its actions; and
- Technology is interpretively flexible due to the interaction between technology and organisations. Different actors from institutions interact differently with technology by using and developing facilities.

The components of the ST model of technology or dimensions of DoT are shown in Figure 2.1 and include:

- Human agents, who are the employees and other relevant users of information;
- Technology, which refers to the facilities and materials that facilitate the usability and execution of tasks; and
- Institutional properties of an institution, referring to the structural management, strategies, culture, control and monitoring measurement, policy, rules, operations and communications.

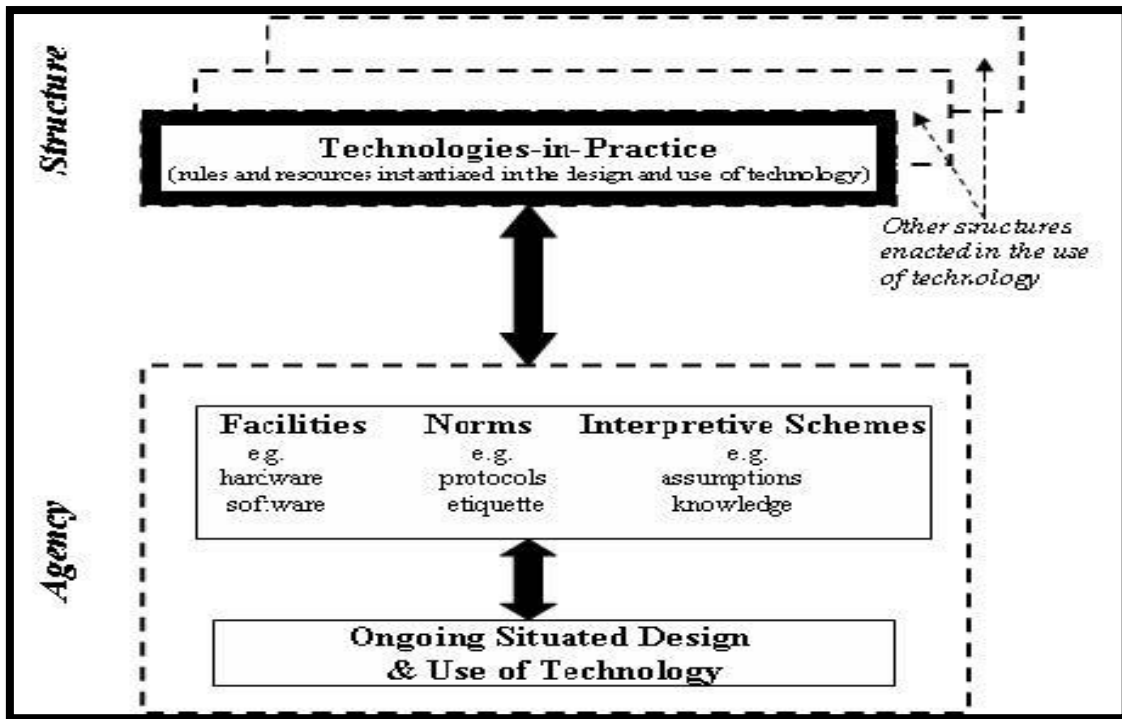


Figure 2.1: Extended enactment of technologies-in-practice model
 [Source: Orlikowski (2000:410)]

2.8.2 Human Agents

In the context of this research, the human agents are the employees and other relevant users of the information. The agents are the actors; their actions produce and develop social structures, which enable them to perform various tasks. ST enables interactions between employees and the technology used in order to produce an outcome. The relationship is established in terms of usability, processes and interactions between employees and technology.

The human agents have the power to use resources or technology and - in practice - the human agents have the transformational capacity to change the society, to innovate and to bring an input to the community.

Within this study, employees are the technical agents, who are working for an institution; they bring an input and they have the capacity to transform the institution. Employees have the power to use institutional resources and, according to Rose and Scheepers (2001), agents have an effect on the resources and can produce unintended results.

2.8.3 Technology

Technology refers to the facilities, resources, instruments, tools or materials that facilitate the usability and execution of tasks. It is used as a medium and product of human action. According to Giddens (1984), resources are the tools or instruments designed and reproduced by human agents during the course of interaction; these resources facilitate the execution of tasks. Also, Orlikowski and Baroudi (2000) stated that technology is an outcome of human action through innovation, concept, modification and process. In the context of this study, employees use technology as a medium to capture, communicate and process information from both inside and outside an organisation. However, technology facilitates and constrains employees' actions through usability and norms.

2.8.4 Institutional Properties of an Organisation

Institutional policies include structural management, strategies, culture, control and monitoring measurement, policy, rules, operations and communications. Institutional properties can influence an employee during his or her interaction with technology and has many benefits, including intentions to comply, awareness, skills, norms, knowledge, incentives and security of information. On the contrary, there are consequences related to the interaction between employees and technology, such as leakage of information, cyber theft, fraud, corruption and other types of security breaches occurring in real time. As such, the interaction with technology can influence the institutional properties to reinforce security measurement, strategies and policies or transform the structures of signification. According to Elbasha and Wright (2017), this construct identifies issues, addresses them and establishes a relationship between different actors within a network. In other words, the structuration model of technology develops a link between the individuals, technologies and the different institutional levels, through practices within their environment and institutional structure.

2.8.5 Structuration Model in Practice

Structuration is the process that involves diverse interactions with technology, which may shape and be shaped by the new structure of an organisation (Christopher & David, 2014). Structuration establishes a connection between human actors, technology and the institutional properties of an organisation at various levels. In the context of this research, structuration helps to determine how InfoSecPol can be enforced, in order to determine the factors that cause information leakage in an organisation and to determine the factors that influence InfoSecPol compliance. The focus is on securing information and information resources through compliance with policies. This led to

the building of a proposed general framework, which could be used to manage the InfoSecPol compliance in an organisation.

2.8.6 Structuration Theory: Duality of Technology

DoT includes structure and agency, where these two concepts are co-dependent. In duality, social structure and human interaction are divided into three dimensions, explained by linking the processes of structure, modality and interaction. The use of security practices becomes legalised within organisations. According to Giddens (1984), the duality of structure uses security practices to form the structural properties of organisations, which are designed by human actors during their interactions (agency). Thus, the use of practice in turn reinforces the structural properties.

This study used the dimension of the DoT as a lens through which the data was viewed and interpreted by paying attention to what, whom, how and why. This will be further discussed in Chapter 4. According to Stones (2014) and Elbasha and Wright (2017), the duality of structure is an ontology that relates to particular social processes and events in a specific time and place. In other words, this can move us to “who did what, how and why”, which means that duality is based on the reality in existence.

The reality is that institutions have existing policies, rules and guidelines on IS. On the other hand, information is frequently leaked by employees in institutions and other relevant users of information. Therefore, for study purposes, the use of the structuration model of technology guided the data analysis by determining how InfoSecPol was enforced, investigating the factors that influence non-compliance with InfoSecPol and determining the factors that influence compliance with InfoSecPol in an institution.

2.9 SUMMARY

The literature review has shown how ICT brings about a change in the lifestyle of a community through how people work, communicate, do business, learn and live. The presence of ICT acts as a platform to enable communication between people in real-time, through the use of the Internet. Also, ICT has changed society, as people are moving from face-to-face communications to the digital space. Conversely, ICT has faced several adoption challenges, as institutions are not able to purchase ICT facilities due to the high costs of the hardware, software and maintenance. Also, ICT has generated cybercrime, fraud, theft and corruption on the Internet, causing challenges for organisations and people. Cybercriminals are using technologies as a medium to leak information from targeted organisations.

IS, in its nature, starts with a basic understanding of risk and how to manage those risks. In some way, IS makes employees aware of the organisational structure and security threats, and gives employees an understanding of how to identify the risks and keep information secure. Organisations need ongoing IS awareness in order to minimise the risk of information leakage and to enforce InfoSecPol compliance.

A service can be a valuable action, accomplishment or it can be an effort performed to satisfy a need or to achieve a demand. Organisations provide services to their clients and partners that are either profit-oriented or for non-profit. Different institutions employ various approaches in the implementation of their IS policies, which can be derailed due to factors such as security breaches. Awareness makes people keep information assets safe.

Institutions need Policy Compliance for regulating employees' information, security behaviours and safeguarding information resources from abuse and leakage. Various studies have emerged explaining the importance of employees' compliance with the policy as a useful technique, which influences the behaviours of their employees on how they protect information. Several factors, such as awareness of policy, communication about the policy and good management skills, are employed to enforce policy compliance. Employees' lack of compliance with InfoSecPol and lack of management skills are the causes of security breaches in institutions. Employees are the key reasons behind problems with IS, based on unawareness, lack of implementation of policies, insufficiency of resources, carelessness or a lack of incentives and poor management skills, through a poorly designed InfoSecPol. This study used ST as a lens through which the data was viewed and interpreted.

The next Chapter will discuss the research approach.

CHAPTER THREE: RESEARCH APPROACH

3.1 INTRODUCTION

The previous Chapter reviewed the literature supporting this study, which included ICT, institutional services and institutional management, information leakage, information policy and policy compliance. Furthermore, the Chapter discussed ST as a lens through which the phenomenon was viewed and the collected data interpreted. This chapter discusses the research design in Section 3.2, research techniques and procedures used in Section 3.3, unit of analysis in Section 3.4, data collection in Section 3.5, data analysis in Section 3.6, data quality assurance in Section 3.7 and ethical consideration in Section 3.8.

3.2 RESEARCH DESIGN

Drawing from the work of Yin (2009), the research design of this study was to logically connect the research purpose and questions to the process for empirical data collection and data analysis, in order to draw conclusions from the data collected. The design relies on the chosen interpretive research paradigm using a case study analysed through qualitative methods (Creswell, 2009). An interpretive qualitative case study was the ideal strategy, as it focused on a real-life setting, which provided an understanding of the meaningful characteristics of the actual situations, such as an individual's life, and institutional and managerial processes (Zikmund *et al.*, 2010). According to Patton (2002), the underlying principle in selecting appropriate cases is the preference for information-rich cases - with respect to the topic under investigation - resulting in the use of purposive sampling. As indicated in Chapter 1, this research study was based on case studies from CPUT and VU; within these cases were the units of analysis, namely the HR department and the Administration office. The study used a semi-structured face-to-face interview method to question the participants, so that they could express their views and opinions, in order to collect the necessary data. The participants were selected based on criteria such as positions, roles and responsibilities assumed within the departments. The objects of analysis were HR managers, administration managers, strategic managers, secretaries, assistant managers and other staff working within the selected departments.

3.3 TECHNIQUES AND PROCEDURES

Determining the data collection techniques and procedures is one of the strengths of the case study method, because of its flexibility and adaptability. The techniques and procedures allow single or multiple methods of data collection to be used when investigating a research problem

(Cavaye, 1996). This study used techniques and procedures which includes sampling, data collection and data analysis techniques.

3.4 UNIT OF ANALYSIS

For this research study, CPUT and VU were used as the main units and within the main units, departments such as HR and the administration office were used as sub-units (in the analysis of the data).

Sampling Technique

This research study used non-probability sampling because it is the preferred method for qualitative studies, as it uses a non-numerical method of generalisation (Yin, 2011). The reasons for selecting participants from these two departments were based on the following criteria:

- i) these two departments have key roles and positions;
- ii) they maintain and improve the university's policies;
- iii) they deal with the students' results; and
- iv) they manage and keep university information.

Therefore, the researcher wanted to understand the meaningful characteristics of the actual situations happening within the institution; this included HR managers, administration managers, strategic managers, secretaries, assistant managers and other staff working within the selected departments.

3.5 DATA COLLECTION

In this study, the researcher used semi-structured interviews as it gives the interviewee an opportunity to explain and provide more information based on the phenomena of research. Also, the study used documents from the selected institutions in order to support the collected data from the interviews.

3.5.1 Interviews

Semi-structured interview techniques were used to question all the participants, as they could express their views and opinions. The interviews were conducted at the participants' office(s). The semi-structured method has both structured and unstructured features, thus both closed and open questions were used. This type of interview has a set of pre-planned core questions for guidance, such that the same area is covered with each interviewee.

3.5.2 Documentation

Documentation, as described in this study, is part of the secondary data, meaning that the data has been collected and evaluated by another person. According to Kotlar and Massis (2014), the secondary raw data helps to retrieve the correct information for the study. Thus, available information from the selected universities' brochures and websites were accessed to collect information to support the data provided from the interviews.

3.6 DATA ANALYSIS

Qualitative data analysis involves "working with the data, organising them, breaking them into manageable units, coding them, synthesising them and searching for patterns" (Zhang & Wildemuth, 2009). The purpose of qualitative data is to discover patterns, concepts, themes and meanings. The process of data analysis starts with categorisations and then organises the data into search patterns, critical themes and meanings that emerge from the collected data (Braun & Clarke, 2013). In this study, the interviews were recorded and transcribed so that the researcher could analyse and describe the data separately for each participant (based on his or her experiences, views and perspectives on the phenomenon). The interview responses were compared, categorised and then triangulated to help with interpretation, in order to draw conclusions.

The study followed qualitative content analysis and interpretive analysis methods for analysing the data:

- i) Qualitative content analysis was followed to analyse documentation, such as brochures and information obtained from the websites of the case study universities; and
- ii) Interpretive analysis was followed for analysing the words of the participants, using the semi-structured interview method.

3.6.1 Qualitative Content Analysis

For this study's purposes, qualitative content analysis was chosen for analysing the documentation and information obtained from the websites of the case study universities. The process included the analysis of the obtained information and creation of categories as the researcher was reading the information, understanding it and rewriting it into text. Thereafter, it was subjected to qualitative content analysis where designs and themes, inductively, were identified from the information obtained (Wahyuni, 2012). Inductive content analysis is an analysis of qualitative data by splitting data into small chunks that allow for sense making (Babbie & Mouton, 2011).

The following process was used during the qualitative, inductive, content analysis (Zhang & Wildemuth, 2009):

- i) Information transcription into written text;
- ii) Comparing and opposing of information obtained from different documents and websites of the case study universities;
- iii) Putting together information to analyse and define the unit of analysis for the process;
- iv) Development of categories and units of analysis orders (this was done inductively from the information obtained);
- v) Analysing all units;
- vi) Evaluating units of analysis;
- vii) Selecting important categories to fit into the theoretical framework;
- viii) Drawing a conclusion from the analysed information; and
- ix) Reporting on the analysed information.

3.6.2 Interpretive Analysis

Interpretive analysis is an experiential analytical method that focuses on the words of the participants (Braun & Clarke, 2013). It aims to provide an understanding for a given person and context, by making sense of a given phenomenon (Braun *et al.*, 2013). In addition, interpretive analysis focuses on a participant's experience, which has implications for how an individual identifies in a specific context (Pietkiewicz & Smith, 2012).

For the purpose of this study, interpretive analysis was followed to gain an understanding of how InfoSecPol compliance could be managed in institutions, identifying the factors that influence non-compliance, identifying and understanding the factors that influence compliance, and understanding how the InfoSecPol could be enforced in institutions.

The interpretive analysis was concerned with interpreting the meaning of the authentic experiences of the employees, for the selected universities or cases. The researcher set aside his prejudgments, intuition, imagination and other general structures to get an insider's viewpoint (Pietkiewicz *et al.*, 2012).

For this study's purposes, the interpretive analysis procedure included:

- i) Transcription of the data;

- ii) Reading and understanding of the data;
- iii) Writing down the information;
- iv) Developing emergent themes;
- v) Identifying the connections across emergent themes; and
- vi) Interpreting the data.

3.7 DATA QUALITY ASSURANCE

According to Saunders *et al.* (2009), data quality must follow a quality standard, validity and reliability. For this study's purposes, the data quality was taken into consideration and followed a quality standard that was valid and reliable.

3.7.1 Data Validity

The interview questions were accurately measured. The title, aim, summary and themes of the study were sent via email to the participants before the day of the interview, to enable the participants to be prepared by obtaining the supportive documents.

The following steps were taken to ensure the validity of the collected data:

- i) Data collected was from VU and CPUT;
- ii) The interview date and time were selected to make sure that procedures did not influence the data collection process; and
- iii) Interview questions were both pre-tested and pilot tested before the in-depth interview with the participants was conducted.

3.7.1.1 Pre-test

According to Burke and Miller (2001), the pre-test phase addresses issues that need to be worked out before the data collection process. A pre-test interview was carried out with an HR assistant manager and then with an administration assistant manager. The idea was to make sure that the list of designed interview questions was correctly interpreted by the participants. This helped the researcher to eliminate some possible problems related to the interview questions and the way of conducting the interviews.

3.7.1.2 Pilot-test

After finishing with the pre-test phase, a pilot study was performed with an HR assistant manager and administration assistant manager, where the researcher asked the participants to provide brief comments based on the interview. The participants confirmed to the researcher that the questions

were appropriate and the correct data would be captured. A few adjustments were made to the interview questions, which led to their final arrangement.

3.7.2 Data Reliability and Conformability

According to Zhang and Wildemuth (2009), data reliability and conformability is established through reviews of the research process and findings. Reliability can be determined by verifying the consistency of the research process, while conformability can be determined by verifying the relationship that exists between the data, findings, interpretations and recommendations (Zhang & Wildemuth, 2009).

In order to ensure the data reliability and conformability through this research study, a full description of the participants was made available on a compact disc (CD), which contains the recorded interviews. The findings from the data analysis helped to propose a general framework, which can be used to manage InfoSecPol compliance in institutions; thereafter, transcribed notes were attached to the thesis.

3.8 ETHICAL CONSIDERATION

The participation in this research study was voluntary, and participants were free to withdraw from the study without any consequences. The study excluded participants who could not give consent. The research study has not involved any processes that could cause harm to the participants or to the environment; all the participants were treated with respect.

According to Babbie and Mouton (2001), ethical consideration of research is recommended to ensure the confidentiality and anonymity of participants during the research period. To this effect, an ethical clearance letter was obtained from the CPUT's ethics review committee and permission from both selected universities were provided for the data collection.

3.8.1 Ethics and Consent

This research study ensured that the rights of the selected universities and their staff members were maintained. Also, the collected data was presented without manipulation of results, in agreement with the standards of the Faculty of Informatics and Design, CPUT Research Ethics Committee.

The data collection techniques, aims and objectives of the study were explained to the participants before an agreement was made. The time and date to conduct interviews were chosen and the

interview themes were sent to the participants before the interview date, in order for them to prepare. Finally, participants signed an informed consent form that described their rights to participate and withdraw from the study before being recorded. Accordingly, the information obtained was kept anonymous and confidential.

3.8.2 Confidentiality

In order to protect the rights and identity of the participants, anonymity and confidentiality were used within this study through the use of pseudonyms. The researcher explained to the participants that the requested information was needed for academic purposes such as thesis, articles and conferences and could not be used against them. However, the information obtained could be useful for affected institutions to recommend a developmental framework, which could be used to manage InfoSecPol compliance.

3.9 SUMMARY

This Chapter introduced the research techniques used to achieve the objectives of the study. The design and methodology that guided the researcher on how to obtain the knowledge within the study was analysed. The Chapter defined ontology as the reality that exists, while epistemology is the knowledge about that existing reality and knowing how those realities exist.

The research design that was followed in this study was an interpretive case study, that was analysed through qualitative methods and applied by selecting the universities CPUT and VU as case studies. Within these main units, the sub-units that were used in the analysis of the data were the HR department and the Administration office. The next Chapter will discuss the data analysis.

CHAPTER FOUR: FINDINGS AND INTERPRETATION

4.1. INTRODUCTION

The previous Chapter presented the research design and methodology this study followed and provided a clear understanding about ontology and epistemology research. This Chapter, therefore, elaborates on the data analysis, findings and interpretation. This study is qualitative in nature and engages an interpretivist method. The implication therefore is the use qualitative approach for data collection to address the research objectives. Additionally, this Chapter presents methods and procedures on how the data analysis progressed and identified categories and themes after the analysis. This Chapter goes into detail on the results derived from interviews performed with Human Resources managers, administration managers, assistant managers and secretaries, operating in the selected University in the Western Cape, South Africa and a European University in The Netherlands, Amsterdam.

The analysis of data was in respect to the research questions asked and relation to the themes generated from interviews. The duality of structure of ST concept guided the classification of the themes identified through the findings and interpreted to revise the conceptual framework. The outcome of this analysis - and the findings led to the proposed general framework as the revised conceptual framework.

4.2. PROCESS OF ANALYSIS

4.2.1 Overview of the methodology

Drawing from Myers (1997), primary objective for adopting a qualitative approach to this study is to understand and explain the social phenomenon of the perception of employees concerning information security policy compliance in an organisation. Drawing from the work of Anderson (2010), this qualitative study included collecting, analysing and interpreting the data that answered the research questions, through the lens of the underpinning theory.

This study used an interpretive qualitative case study as the research approach, which facilitated the exploration of phenomenon within its context using a variety of data sources. Therefore, the issue was explored through a variety of lenses, which enabled different perspectives of the phenomenon to be revealed and understood (Baxter & Jack, 2008; Fouché & Delport, 2011). This was the foundation for the choice of using CPUT and VU for the case studies. An interpretive

qualitative case study method was used to understand employee perceptions with regards to issues of the extent of non-compliance, within an institution's InfoSecPol.

This approach (an interpretive qualitative case study) was adopted in order to focus on actuality and relevance settings, such as an individual's life, institutional processes and international relations. Drawing from Yin (2013), the adoption of the interpretive qualitative case study was to produce new strategies and techniques on how to implement InfoSecPols. The focus was to understand the causes affecting a specific situation and to come up with broad generalisation that depended on the evidence from the cases studied; thus, to propose a general framework to be used to manage InfoSecPol compliance in an institution.

4.2.2 Overview of qualitative analysis

The data obtained from the semi-structured interview methods were subjected to content analysis. According to Rose *et al.* (2015), content analysis is a method applied in qualitative social research that engages processes for methodical analysis of text by using coding patterns.

This research followed content analysis by adopting the following steps:

- i) Ensuing transcriptions of the semi-structured interviews recorded, a careful reading and understanding of the transcript was achieved. Through the reading, ideas relating to knowledge around the themes emerged from the transcript. Additionally, the reading was done repetitively to determine the leading themes;
- ii) Afterward, a worksheet was created in Microsoft Excel, into which each question was set on its own spreadsheet;
- iii) The spreadsheets included describing criteria such as positions, roles and responsibilities assumed within the departments. The intention was to improve the understanding of responses provided by each participant.
- iv) The duality of structure of ST was used to guide the design and analysis of data collection. The study also used the reviewed literature to conceptualize the problem. Therefore, these provided the basis for the coding and generating the themes. For this reason, the coding was used consistently throughout the analysis and interpretation of data;
- v) Also, the modalities of the duality of structure (i.e., Interpretive Schemes, Norms and Facilities) guided the generation of codes from the themes (classified according in order to effectively interpret the research problem);

- vi) The word or collection of words that were associated with the themes were identified in the problem conceptualisation, including any new themes that emerged from the data; and
- The themes developed were influenced by the data. The underpinning theory played an important role by identifying the themes as discussed above.

After a careful reading, a total of six categories emerged from the codes, the interview data, questions in the interviews and common sense constructs. These categories were then made into themes and a total of three themes emerged. These themes were also derived from common sense constructs and theoretical understanding of the phenomenon (Ryan & Bernard, 2003).

Table 4.1 presents the summary of categories and themes that emerged from both selected universities.

Table 4.1: Summary of categories and themes

CATEGORIES	THEMES
1. Information security policies 2. Policy compliance	1. Information Security Policies as interpretive schemes
3. Protection of resources 4. Technology	2. Information Systems and Technology as facilities
5. Attitude towards compliance 6. Responsibility	3. Norms as culture of compliance

4.2.2.1 Overview of the analysis technique

The analysis technique included procedures for obtaining, analysing and interpreting detailed data to be useful in social studies (Patton, 1999). In the context of this study, content analysis had been used systematically for the coding of rich data, and analysed to deliver meanings to the phenomenon of the study. Since the objectives of this study were to:

- i) Determine how InfoSecPols are enforced in an institution;
- ii) Investigate the factors that influence non-compliance of the InfoSecPol in an institution; and
- iii) Determine the factors that influence compliance of the InfoSecPol in an institution.

Given the ontological stance to study the phenomenon, and in the context of the concept of duality of structure, content analysis was considered to be more suitable. Thus, from a qualitative perspective, content analysis involved the coding and the creation of categories₇ by grouping similar patterns.

The coding was done manually on a worksheet where the answers to the questions of the semi-structured interviews were captured. Coding was achieved through the identification of the words and phrases that emerged when reading through the responses. Each question's answers were captured into a distinct worksheet and later used the dimensions of duality of structure (interpretive schemes, norms and facilities) to guide the interpretation of the answers.

4.2.2.2 Overview of data validation

As indicated before, the analysis was done by regrouping, summarising and examining the data to obtain findings which addressed, primarily, the objectives of this research (Rabiee, 2004). Furthermore, Thomas (2006) stated that data analysis from an inductive perspective is required to:

- i) Consider diverse raw data into a brief summarised format;
- ii) Establish relations between the research objectives and summary findings derived from the raw data in a way that could answer them; and
- iii) Develop a model or theory with regards to underlying structure presented in the findings.

Therefore, the data analysis for this research study was done using keywords - together with themes - extracted from the rich data narrative, coded, grouped and summarised. They were built on similar categories to provide meanings and answers to reach questions (Gillham, 2000).

The validity of the analysis in this study denotes the degree in which the analysis of the data obtained is reliable (Thomas, 2006). Thus, drawing from According to Anderson (2010), the validity of data was done honestly, with authenticity and genuineness. In the context of this research, validity was achieved by discussing the data collected with the participants (managers, assistant managers and secretaries) for their validation and approval. This ensured that what was answered by the participants during their interviews was exactly what was reported, and revealed in the findings. The intention was to get feedback in order to make corrections. Additionally, validation was achieved by applying triangulation, which involved comparing the data obtained from the interviews to make sure that the findings represented the views of the respondents.

4.2.3 The Case and unit of analysis

This study used universities as a unit of analysis. Two universities were selected: CPUT and VU. Within the main units, the HR Department and the Administration office were used as sub-units in

the analysis of the data. CPUT is situated in Cape Town, South Africa and VU is situated in Amsterdam, The Netherlands. Table 4.2 presents the selected institutions as the main units, their departments as sub-units as well as the place of operation.

Table 4.2: Main and sub-units of analysis

Institutions	Departments	Place of Operation
1. VU	Administration	Amsterdam, Netherlands
	Human Resources (HR)	
2. CPUT	Administration	Cape Town, South Africa
	Human Resources (HR)	

i) Case 1: VU

The English equivalence of the Dutch name, Vrije Universiteit, is "Free University". "Free" refers to independence of both state and church. The institution is usually referred to as "the VU". This university is located in Amsterdam, The Netherlands and has received government funding on an equivalent basis with public universities since 1970. Over the years, VU has changed from a small institution into a broad, research-intensive university attended by a wide variety of students from different backgrounds and the courses are taught in English (VU University Amsterdam, 2015). According to *Leiden Ranking*, VU was acknowledged as the second-best university, nationally.

ii) Case 2: CPUT:

CPUT was established on 1 January 2005, when the Cape Technikon and Peninsula Technikon merged. This unification was part of a national transformation process that changed the higher education background in South Africa. It is now the only university of technology in the Western Cape Province and is the largest university in the region, boasting more than 30 000 students, numerous campuses and service points and more than 70 programmes. Like VU, the courses are taught in English (CPUT, 2015).

4.2.4 Overview of sampling process

The participants were selected based on criteria such as their positions, roles and responsibilities assumed within the departments. This included Human Resources managers, administration managers, strategy managers, assistant managers and secretaries, who all provided good insights. These participants were the most representative people - holding key roles and positions - as they maintain and improve the institution's HR and administration by planning, implementing and evaluating employees' relations and policies, services and practices. They also manage

students' data, as well as preparing and keeping both students and institutional records or information.

17 participants were selected for the process. Participants one to nine were from VU, and were the key university representatives from HR and the administration office (including managers, strategy managers, secretaries and assistant managers). Participants 10 to 17 were from CPUT, and were the key university representatives from HR and the administration office (including managers, strategy managers, secretaries and assistant managers). Table 4.3 presents the selected participants from the departments as sub-units.

Table 4.3: Participants from sub-units

Department	Level of Management	VU	CPUT	Total
Human Resources	HR Manager	1	1	2
	Strategic manager	1	0	1
	Assistant manager	1	2	3
	Secretary	1	1	2
Administration Office	Admin. Manager	1	1	2
	Strategic manager	1	0	1
	Assistant manager	2	2	4
	Secretary	1	1	2
Total		9	8	17

4.3 ANALYSIS AND INTERPRETATION

4.3.1 INTRODUCTION

The previous sections presented the methods and procedures on how the data analysis progressed, and identified categories and themes after the analysis. This section goes into detail on the results derived from interviews performed with HR and administration managers, assistant managers and secretaries operating in the selected universities (CPUT and VU). The dimension of duality of structure was used to categorise the themes identified and to interpret the findings which was used to enhance the conceptual framework. Furthermore, this section discusses the themes and presents answers to the main research question and sub-questions.

The analysis of data was in respect to the research questions asked, exploring the themes obtained from interviews. The outcome of this analysis - and the findings - was used to revise the original conceptual framework to propose a general framework.

4.3.2 Answers to the research question

4.3.2.1 The main research question:

How can the non-compliance with InfoSecPol by employees in an institution be managed?

When this question was asked, the following responses were recorded:

Compliance is achieved when the purpose of the policies is shared in the form of guidelines for its implementation.... therefore, a standard operating procedure facilitates compliance with policies... guidelines direct, guide employees, increase performance and address particular security issues by clarifying the need for IS. (VU manager)

Employees involvement, support and motivation from the management can enable compliance with policies...managers, together with employees, have to establish a line of communication to enable and improve compliance. (CPUT manager)

Similarly, a VU strategic manager added:

It is clear that some proper instructions are considered as effective factors for enforcing employees' compliance in this institution. We then had to come up with procedures and instructions such as training, workshop and conferences about InfoSecPol for enforcing and managing compliance in this institution.

Likewise, a CPUT assistant manager added:

The use of explicit procedures such as awareness, training and guidelines can be considered as effective factors for facilitating compliance with policies.... these factors increase employees' performance and skills needed to manage compliance.

Furthermore, a CPUT manager added:

Availability of facility resources can enable employees to manage compliance with policies.... availability of resources such as offices for lecturers and other facilities can facilitate the management of compliance.

My responsibility and behaviours at workplace are as a set of best practices to manage compliance. (CPUT secretary)

In the same context, a VU assistant manager added:

...knowledge sharing, guidelines, communication and availability of technology influences the specific interests, beliefs and norms to which employees are exposed and managed.

Finally, a VU strategic manager added:

Implementation of a proper monitoring and controlling system through the use of technology, management support and employees' participation can enable the management of compliance with policies.

4.3.2.2 Research sub-question 1:

How are Information Security Policies enforced in the organisation?

When this question was asked, the following responses were recorded:

Employees' involvement, knowledge sharing, communication and training can enforce compliance in an institution..... Employees' involvement can create and sustain policies...policies have been created for employees to comply with. Employees who comply with policies enforce IS and protect information. (CPUT manager)

... Education, social engagement, technology and policies ...but to have policies in place does not guarantee compliance. Therefore, a procedure and guidelines has to be implemented as a mechanism that can influence and enforce compliance with policies by identifying how the knowledge can be shared. (VU strategic manager)

Similarly, a CPUT assistant manager added:

The knowledge management about InfoSecPol and knowledge sharing can enforce information security in this institution...The knowledge management instructs and increases knowledge about information security.

Furthermore, a VU manager added:

Employees' contribution and participation need to be considered because they are the central point of education, knowledge sharing and compliance with policies. They are acting as a medium between knowledge and compliance.

Also, a CPUT manager added:

In terms of lines of communication and knowledge sharing, employees play an important role. This is because security strategies such as policies, operating procedures, awareness and other security features are created, used and enforced by employees.

Finally, a VU secretary added:

For me...Technology and social engagement enforce compliance with policies...human social engagement may generate trust to engage in knowledge sharing...also, the use of technology can enable the learning process and knowledge sharing by enabling a line of communication between employees, to enforce compliance.

The findings revealed that InfoSecPols are enforced through human involvement, the use of policies, standard operating procedures, organisational culture, education, knowledge sharing, social engagement, lines of communication, management support and technology.

Given the responses above, it implied that to have policies in place constituted a significant enabler that can set employees' minds on how to share knowledge. Conversely, to have InfoSecPols in place does not guarantee compliance. This is because it is assumed that the implementation of InfoSecPols alone does not influence employees' compliance; therefore, concluding that policies in themselves cannot require employees to comply. Thus, standard operating procedures were identified as a mechanism that could efficiently influence and enforce compliance with policies.

Additionally, employees' involvement needs to be considered because, without human capital, the share of knowledge and compliance would not occur. Employees are considered as central for the success of compliance with policies in an organisation. That is, without employees' participation, policies and standard operating procedures or organisational structures would not exist, as these are demonstrations brought by human participation. The outcomes revealed that employees' involvement can be seen as supportive - and as an enabler - for enforcing compliance. According to Fathi *et al.* (2011), employees' involvement generates a suitable atmosphere through lines of communication and knowledge sharing. Furthermore, Reagan and Mcevily (2015) argue that employees' involvement contributes to the creation and maintenance of policies.

4.3.2.3 Research sub-question 2:

What are the factors that influence non-compliance with InfoSecPols in an institution?

When this question was asked, the following responses were recorded:

...for me, the factors that influence non-compliance with IS policies include a lack of awareness, insufficiency of knowledge and insufficiency of resources. (VU manager)

...fraud, theft, lack of education and lack of transparency. (CPUT manager)

Similarly, an assistant manager from VU added:

...the factors that influence non-compliance with InfoSecPols include misuse and abuse of facilities and poor implementation of guidelines.

In the same context, a CPUT secretary added:

...We are facing challenges of a different nature, including the low level of education, favouritism, lack of leadership skills and corruption...Some of the challenges are due to the insufficiency of resources and a lack of management support.

Also, a CPUT assistant manager added:

...the factors that influence non-compliance with InfoSecPols include incentive issues, poverty, inequality, inexperienced staff members, and so on.

Finally, a VU strategic manager added:

...the factors that influence non-compliance with InfoSecPols include the inadequate social environment and the lack of social norms.

The findings of this study revealed some factors that influence non-compliance with InfoSecPol, including a lack of awareness, training, education, misuse and abuse of facilities, insufficiency of resources, fraud, theft, corruption and a lack of transparency, lack of leadership skills, poor implementation of norms and values, incentive issues and inexperienced staff members, among others. The outcomes revealed that institutions are facing challenges of a different nature, including the low level of education, an inadequate social environment and the lack of social norms. Some of the challenges are due to the lack of knowledge about InfoSecPols, insufficiency of resources and lack of management support.

Moreover, the findings revealed that the factors of non-compliance with InfoSecPols have serious consequences to an institution, including an inability to:

- i) sustain institutional goals and objectives:
- ii) carry out the service effectively and efficiently;
- iii) compete in the industry or market; and
- iv) manage the activities of the institution.

Thus, these consequences sometimes led to job losses or an institution's closure.

4.3.2.4 Research sub-question 3:

What are the factors that influence compliance with InfoSecPols?

When this question was asked, the following responses were recorded:

...the factors that influence compliance with InfoSecPols include management support, mandate, training, performance management and knowledge sharing among employees. (VU manager)

.... the factors that influence compliance with InfoSecPols include education, awareness, leadership skills, governance and communication. (CPUT manager)

Furthermore, a VU strategic manager added:

...According to me...the factors that influence compliance with InfoSecPols include availability of resources, technology, organisational culture and management support.

Similarly, a CPUT assistant manager added:

The factors that influence compliance with InfoSecPols include education, workshops, knowledge sharing, performance management and service delivery.

In the same context a CPUT secretary added:

...we need a proper service delivery; equality, transparency, reliability and good governance.... also, educate employees.

Finally, a VU secretary added:

The factors that influence compliance with InfoSecPols include honesty, responsibility, commitment and good behaviours in practice.

In the context of this study, the main factors that influence compliance with InfoSecPols include governance, standard operating procedures, education, awareness, leadership skills, technology, organisational structure, management support, mandate, performance management and knowledge sharing. The findings revealed that these factors enable proper policy alignment for the improvement of InfoSecPol compliance

Given the responses above, it is certain that the factors relating to management support enables compliance of policies, which creates dual reporting lines between managers and employees. In light of this, management support enables the establishment of a set of moral behaviours and belief needed by making lines of communication more effective. Moreover, these compliance factors influence and motivate employees to engage more with knowledge IS.

Furthermore, the outcomes revealed that organisational culture is an important factor that influences compliance with policies. It is evident that organisational culture drives the norms

needed for management knowledge sharing in the institution. Finally, a factor such as governance was identified as an important factor for the types of normative sets of values that can drive the share of knowledge from an institutional perspective. It is perceived as a set of best practices that drive all knowledge management strategies influencing compliance with policies.

4.3.3 Factors of Interpretive Schemes for Information Security Policies

The role of the interpretive scheme is in shaping peoples' actions. According to Giddens (1984), interpretative schemes are the routines of knowledge that enable actors to understand things, whether they are physical, abstract or conceptual. This understood knowledge is obtained through experience. In other words, interpretive schemes are the rules that facilitate the understanding of what to know, while norms are understood as the rules for understanding how to act (Walsham, 2002).

An interpretive scheme about technology includes the following aspects: policies and beliefs about what the technology is, policies and beliefs about why the technology has been adopted, and policies and beliefs of how the technology could and should be used. The interpretive scheme is a modality that is used to produce and reproduce the structure (in this case, IS in practice), in the interplay between the actors.

Interpretive scheme has the role of both enabling and constraining effects (Yoshioka *et al.*, 2002). On the one hand, interpretive scheme is enabling as it guides organisational action, allowing interpretation of difficult situations, and reducing uncertainty in conditions of complexity and change. On the other hand, interpretive scheme is also constraining, as it enforces an unreflective trust on knowledge, limits learning and misleads information by making it possible. Employees transmit interpretive scheme to others through training, communication and social interaction. Thus, employees and their participations at the workplace influence the specific interests, beliefs and norms to which they are exposed. It is likewise important to know that interpretive schemes are also known as lines of communication involving the application of policies and regulations that include people, standard operating procedures, information systems and institutional structure.

Policies play a significant role in the institutionalisation of sharing knowledge and compliance in an organisation. It was predicted that policies would influence employees' compliance through sharing of knowledge in an organisation. The analysis of data affirms this assumption by presenting policies as an important factor that enables compliance, knowledge sharing and communication. Institutions establish policies as rules and instructions, to guide employees and

secure information through compliance. As such, they increase employees' performance, knowledge, skills, protection and compliance with information. This study mentioned that the increase of knowledge is justified by many factors, including communication of the policies, awareness, training, education, leadership skills and motivation from management. According to this study, the policies must be clear, well defined and understandable. Policies must indicate the institution's attitude towards compliance and claim the "information" as the property of the institution.

The policies are based on the governance of an institution - by defining the processes and activities that an institution is engaged in - which need protection throughout compliance. According to Crossler *et al.* (2013), policies are a set of platforms where the security of information is needed. Furthermore, Shih *et al.* (2016) agreed that policies are a set of rules and guidelines that address security issues. They are the integral part of the organisation's objectives, strategy, vision and goals (Brown *et al.*, 2011). In other words, policies establish a structural culture where the creation of environmental awareness and the behaviour of the employees manages the procedures and activities - inside and outside - of an organisation (Rees & Smith, 2014).

The analysis of data obtained from the interviews revealed that most of employees (from both selected institutions) agreed with the findings. Indeed, it was declared that having policies in place encouraged and motivated employees' compliance in an institution. This declaration was made by a VU manager as follows:

We have to implement policies and structure...The vision via the implementation of those policies targets at getting employees' compliance.

Similarly, a VU assistant manager declared the following:

We have a number of policies in this institution that kind of motivate and encourage employees to comply with [them].

The importance of having policies implemented in an institution is confirmed here in terms of creating the condition to share knowledge for compliance. Therefore, policies get employees to be involved, and motivate them to engage with communication and sharing strategies. However, as a VU secretary stated:

We have policies in place in this institution but I do not think that employees comply with [them].

Similarly, another assistant manager (CPUT) added:

Policies exist but I am not aware of them. Therefore, I cannot comply with [them]...Policies do not enforce employees' compliance in an institution.

Adversely, one manager (CPUT manager) added:

Policies exist. They are in place in terms of enforcement and compliance... Our duty is to enforce policies, motivate and encourage employees to comply effectively.

It was suggested that having InfoSecPols in place is very important in terms of motivating and facilitating employees to engage with compliance. This is because policies instruct, thereby increasing the way knowledge must be shared in an organisation. However, in some cases, the respondents felt that policies did not enforce compliance, whereas some felt that policies were aimed at enforcing compliance. Therefore, the data analysis indicated that policies increased knowledge, secured data and motivated and enforced compliance. According to Yang and Wu (2008), managers need active policies to encourage employees in order to share their experience with others. Furthermore, Twum-Darko and Harker (2014) emphasised that having policies and effective guidelines constitutes an important aspect for the increase of knowledge sharing in an institution. As such, policies influence the line of communication as a medium through which compliance is achieved.

4.3.4 Factors of Norms for a culture of compliance

According to Jones and Karsten (2003), norms are modalities from the dimension of legitimation. This framework of modality provides morality; thus, it includes a set of values and ideas, normative rules, codes of conduct, mutual rights and obligations. Furthermore, Twum-Darko (2014) stated that a structure of modality is a set of ethical codes, leadership, understanding and validation for human interaction, which produces legitimation. Therefore, the factors below were acknowledged

as enablers of the modality of norms, including aspects of support, performance management, organisational culture and governance.

4.3.4.1 Management support

It was suggested that management support enables compliance with respect to policies in the institution. The outcomes from the interviews shown that management support was considered as a significant social enabler for compliance with policies in an institution. This finding is confirmed in the comments made by a VU strategic manager:

Management support controls and directs all the security strategies needed to improve compliance.

Along the same idea, another VU strategic manager added:

There is also a need for communication between management and employees to facilitate the understanding of the importance of compliance with policies.

Similarly, a CPUT secretary added:

Management support develops a strategic executive ability to provide knowledge of IS and enforce compliance amongst employees.

The role of management support is to establish norms for compliance in an institution. By having effective lines of communication between managers and employees, an effective compliance can be achieved and an appropriate set of normative rules for policies can be communicated efficiently. As such, management support is perceived as a significant enabler for compliance. According to Lin (2006) and Twum-Darko and Harker (2015), management support can be perceived as an important element for the effectiveness of knowledge sharing in an organisation. Lin (2007) has mentioned that support from management influences employees' willingness to both collaborate and share knowledge with others. This means that management support identifies norms and practices that are barriers to discussing complex issues. It involves institutional culture, policies, guidelines and procedure implementation. Also, it encompasses security strategies considered as important to compliance (Shorunke *et al.*, 2014).

4.3.4.2 Performance management

The outcome from the data analysis revealed that performance management establishes the norms or moral codes for compliance with policies. This finding is evident in the comments made by a CPUT manager:

Performance management drives norms in terms of compliance with policies... Also it is a driver for norms in terms of knowledge sharing amongst employees.

Similarly, a VU assistant manager added:

Performance management influences lines of communication and enables compliance with policies in an institution.

Performance management can positively impact employees' compliance with policies. The outcome from the interviews revealed that performance management constitutes an effective tool to encourage employees to work together, share knowledge and comply with policies. As such, employees must be evaluated and compensated based on the degree to which they engage with education, skills, experience and knowledge sharing with others. In this context, performance management is an enabler that seeks to encourage and motivate employees to engage with the learning process, knowledge sharing and training in an organisation. Thus, performance management is a driver for Norms in terms of skills, education, communication, knowledge sharing and compliance with policies.

4.3.4.3 Organisational culture

The analysis revealed that organisational culture plays an important role towards establishing compliance with policies. The organisational culture promotes security of information by enabling compliance. The suggestion is that organisational culture is important for securing information in the institution. Majority of the respondents, however, said that they are unaware of the existence of a culture in their institutions. Some of the respondents believes that an organisational culture was important for sharing security knowledge in an institution. The results confirmed that there was a relationship between organisational culture and compliance with policies. This means that

an organisational culture has an impact on knowledge sharing, skills and lines of communication. All these factors motivate and influence employees' compliance with policies. This was affirmed by comments made by a VU assistant manager:

Organisational culture is based on knowledge sharing, learning process, and line of collaboration...Some organisations succeed well because it is built into their culture but [for] others it is not, because of different reasons.

I am sure that we are trying to create [a] security culture and share our knowledge with others, [to] help others to understand the importance of compliance with policies.

In the same context, another VU manager added:

Some private organisations use their organisational culture for competitive advantages. They use their knowledge management to compete with others. They learn new things and share with others.

A CPUT manager added:

We can suggest new security strategies, share the security knowledge to enforce knowledge sharing from a cultural point of view but the reality is that every employee in this institution is supposed to share what he/she knows. The knowledge sharing increases security and [leads] to compliance with policies.

It is evident from the above comments that a culture for sharing knowledge increases employees' performance and leads to compliance with policies. Most of the respondents believed that organisational culture knowledge sharing was suitable in the private sector (for competitive advantage). Furthermore, since they operate in public institutions where they do not have competitors, they are more focused on service delivery. These respondents felt that a culture of sharing knowledge is also appropriate in the IT departments, or is appropriate for IT people in terms of security strategies, skills and compliance. Nevertheless, through detailed analysis the

comments above, it was found that a culture of sharing knowledge does not exist within their organisations. Organisational culture of sharing knowledge to improve security approaches and techniques of information security includes the improvement of certain practices in an organisation. The findings revealed that the use of various mechanisms such as policies, technology, management support and organisational culture can influence employees' compliance.

The above results confirm the perceptions of Jonsson and Kalling (2007), who stated that organisational culture facilitates the flow of knowledge, policies, technology and other sets of practices. Similarly, Ju *et al.* (2010) declared that organisational culture can be considered as an enabler for knowledge sharing and facilitates an environment for interactions between employees, and that it improves relationships amongst employees. According to Huang *et al.* (2013), organisational culture defines appropriate structures of governance, leadership and support from the management within the institutions. It impacts on the moral codes required to enable compliance with policies.

4.3.4.4 Governance

It has been identified that governance is a major factor for the improvement of compliance with policies in an organisation. That is governance is considered in this research as set of techniques needed for the improvement of compliance with policies. This was affirmed by comments made by a VU manager:

Governance is a set of best practices needed for the improvement of compliance with policies.

In the context of our institution, we need to have governance...we have to show the importance of policies. If we are mandated, we may have the power to impose and direct how compliance should be implemented, established and shared in the institution.

Similarly, a CPUT manager added:

Governance enables the structure of compliance with policies through the involvement of both manager and employee...This can allow the type of moral values and beliefs needed to address issues of compliance.

Governance contains several aspects, such as the role of governance in relation to governing compliance within an institution. Another aspect is that governance is primarily technology-based. As such, all governance processes including norms, rules, policies, people and communications were used to ensure that compliance would be operative through technology. The outcomes revealed that governance ensured best practices of policies and other security strategies. Also, the outcomes revealed that management support, organisational culture, governance and performance management have been presented as core factors for a culture of compliance. This means that those factors can enable employees' compliance with policies, although governance has not been adequately implemented within the departments of the selected institutions.

4.3.5 Factors of Facilities for Information Systems & Technology

This section discusses the importance of a technology infrastructure for the improvement of compliance with policies. The technology aspect protects, enables and ensures the security of information through compliance. Having technology in place enforces the policies by reducing the risk of violation. Employees have to work together with technology in order to ensure protection of information through compliance. The outcomes revealed that the implementation of information systems enabled the controlling and monitoring of the procedures engaged in within an institution. The prospect of this declaration was confirmed, based on the respondents' comments when they were asked how they felt about the importance complying with information systems' policies, the VU manager narrated as:

I think that the use of information systems is an important means of compliance with security policies.

Clearly it indicated that having information systems, represented in terms of software and information technology infrastructure to facilitate and improve security of information, can have an influence on employees' compliance in the organisation. This declaration is evident in the following comments made by a CPUT manager below:

Technology enables a learning process where employees are exposed to technical and theoretical skills on IS threats...technology enforces and maintains compliance through the lines of knowledge sharing.

The institution must use technologies such as email filters and URL blockers to avoid intentional or unintentional breaches.

It is evident that information systems are presented through the means of technology infrastructure, including an intranet, which is an ICT. Through the information systems, employees are able to share knowledge through the lines of communication in the institution. Information systems are considered by employees as central to fulfilling their responsibilities in terms of lines of communication and the knowledge sharing process. This is evident in the following declarations made by a VU strategic manager:

The institution has to put a good mechanism in place that enables the learning, communication and knowledge sharing process. Our vision for information systems is that we want to build knowledge which is based on technical and theoretical skills. We want to ensure that all the processes, strategies and security skills are shared amongst employees in order to enforce compliance with policies.

The above comments revealed that information systems are considered by employees as important, in order to enable their knowledge management, learning processed, education and communication. The information systems were found to be important as they provided technical and theoretical skills to employees. This included explicit knowledge such as documents, policies, and standard operating procedures. The information systems also included other features, such as software, hardware, data and telecommunication tools that were accessible to all employees in the institution. Therefore, information systems embody an interpretive scheme that enable collaboration between employees, thereby promoting communication.

Technology drives compliance in as much as operating and controlling the access to resources in the organisation. The outcomes revealed that the use of information systems was suggested to be a fundamental means of employees' compliance. Explicit knowledge such as policies, standard

operating procedures and other lines of communication can be shared amongst all employees, enabling knowledge, skills, education and facilitating communication between them.

The use of information systems makes it an important determinant for the enforcement of compliance with policies (in practices within the institutions). These findings confirm the point of views of Sutz *et al.* (2014), who discussed that technology has enabled the opportunity for education and interaction between people and institutions. Furthermore, the outcomes confirm the arguments made by Da Veiga and Martins (2015), who stated that information systems enable a learning process where users are exposed to technical and theoretical skills on IS threats. Thus, they said, the security of information is enforced and maintained. Institutions must implement information systems to protect their operations and processes, which must include all security aspects such as physical security, operational, communication and technology (Whitman *et al.*, 2012).

The DoT is explored to understand the relationship between technologies and human actors in order to ensure security of information. Individual actions are determined neither by technology, nor by lack of knowledge, about technology. The technology itself cannot provide security of information; thus, the combination of human beings and technology is a key factor to prevent security issues. Through the use of technology, several benefits combine to contribute significantly to employees in engaging with compliance, including fast access to information, knowledge sharing, communication, education and integration. This indicates that employees, by using power and domination of the concept of duality of structure, enact and sustain better human management and resource allocation by using technology.

4.4 INSTITUTIONALISING INFORMATION SECURITY POLICIES

4.4.1 INTRODUCTION

Institutionalising InfoSecPols involves the enactment of structural management in practice; thus drawing from the concept of the duality of structure/technology as a lens through which to address the objectives of this research. The findings were generated from a qualitative perspective and categorized according to the modalities of the concept of duality of structure/technology.

According to Orlikowski and Robey (1991), ST is a lens through which the relationship between human actors, technology and organisational structure can be understood and in the case of

information systems security, determine the interplay between the actors. Furthermore, Orlikowski (1992) also applied this interpretation to adapt Giddens' (1984) duality of structure (technology), in order to understand it in the context of IS. In light of this, Orlikowski's (1992) theory extends ST into the real application of technology in organisations, to emphasising on the impact technology and the interaction between people, technology and institutional structures in an organisational context (Pham & Tanner, 2015). According to Larsson (2012), the duality acknowledges technology (Information Systems) as a social product produce and reproduce by human action within certain structural contexts.

In the context of this study, Norms is acknowledged as best practices. It drives structural management to compliance of policies through support and performance from management, organisational culture and governance. These factors enforce moral values and beliefs needed to enforce compliance.

The role of the interpretive scheme is in shaping people's action. According to Giddens (1984), interpretative schemes are the routine of knowledge that enable actors to understand things, whether they are physical, abstract or conceptual. This understood knowledge is obtained through experience. In other words, interpretive schemes are the rules that facilitate the understanding of what to know, while norms are understood as the rules for understanding how to act (Walsham, 2002).

Interpretive schemes about technology includes the following aspects: policies and beliefs about what the technology is, policies and beliefs about why the technology has been adopted, and policies and beliefs of how the technology could and should be used. Interpretive scheme is a modality that is used to produce and reproduce the structure (in this case, IS in practice), in the interplay between the actors.

Interpretive scheme has roles that includes both the enabling and constraining of effects (Yoshioka *et al.*, 2002). On the one hand, interpretive scheme is enabling as it guides organisational action, allowing interpretation of difficult situations, and reducing uncertainty in conditions of complexity and change. On the other hand, interpretive scheme is also constraining, as it enforces an unreflective trust on knowledge, limits learning and misleads information by making it possible. Employees transmit interpretive scheme to others through training, communication and social interaction. Thus, employees and their participation at the workplace influences the specific interests, beliefs and norms to which they are exposed. It is also important to know that interpretive

schemes are also known as lines of communication through the application of policies and regulations, including people, standard operating procedures, information systems and institutional structure.

4.4.2 Policy implementation charter as Interpretive Schemes

Implementation charter or processes involve the standards of procedure for employees which are useful in terms of compliance. They instruct, increase knowledge and support organisational structure within various departments. All these factors enable the enforcement of moral values and beliefs needed for policy compliance. Power which entails the ability of employees to control resource is imposed by policies implementation charter. Thus, human agents demonstrate power to dominate and sustain behaviours around them.

In the context of this study, policies need to be implemented and acknowledged by employees. It is important to know how to effectively implement the policies in the lines of communication with employees. Employees must be advised as to the reasons why the policies are created, what the objectives are, where to find them and how they will be used in the institution. Through the modality of norms, an effective implementation process benefits both employee and institution in terms of the protection of information through compliance with policies.

4.4.2.1 Standard Operating Procedures

It was predicted that standard operating procedures can motivate employees' compliance with policies, and were identified as a significant enabler of compliance. The outcome of the analysis revealed that standard operating procedures enable employees' compliance with policies. The use of standard operating procedures and guidelines is considered a factor that facilitates compliance through the line of communication and knowledge sharing. Thus, the outcome of the analysis of data confirms it as commented below by a VU Human Resources manager:

We are moving toward the implementation of standard operating procedures that have more effective transformation into compliance in the institution.

Standard operating procedures include manuals, guidelines and reports which enable employees' transformation into compliance. As such, standard operating procedures contain instructions

about policies that produce the guidelines on how knowledge sharing can be circulated amongst employees. Therefore, compliance is attained when the object of the policies is illustrated in the form of guidelines for implementation. Actually, standard operating procedures facilitate compliance of policies. As analysis of research data have shown, effective policy compliance is the application of standard operating procedures and guidelines an organisation.

A VU strategic manager, on this subject, stated:

We then had to come up with procedures and guidelines for enforcing compliance in this institution.

Likewise, a CPUT manager added:

The use of procedures and instructions can be considered as effective factors for enabling compliance with policies.

Given the above analysis, standard operating procedures are important enablers for compliance with policies, insofar as they provide the means through which the guidelines are revealed. The data analysis affirms Tohidinia and Mosakhani's (2010) belief that standard operating procedures promote an institutional environment upon which policies and guidelines facilitate employees' compliance. Also, this outcome confirms Babu and Gopalakrishnan's (2008) belief that the use of standard operating procedures in an institution constitutes an important factor through which knowledge is shared (either through a manual or a report).

4.4.2.2 Employees

Employees constitute the centre of knowledge sharing, the lines of communication and compliance with policies. This is because employees can create and maintain policies in the institution. The outcome from the interviews stated that employees' involvement can create and maintain policies as a drive for compliance in the institution. Employees are the centre for compliance. This was confirmed by a VU manager:

Employees' involvement can create and sustain policies...policies have been created for employees to

comply with. Employees who comply with policies enforce IS and protect information.

Another manager from VU added:

Institutions establish policy in order to ensure the security of information resources. Hence, employees have to comply with [the policies].

Finally, a CPUT manager stated the following:

In terms of lines of communication and knowledge sharing, employees play an important role. This is because security strategies such as policies, procedures, awareness and other security features are created, used and enforced by employees.

Employees are a central enabler for compliance in the institution. Employees implement security strategies and share the knowledge with others. Employees are at the core of everything with regards to policy implementation and compliance. The outcomes revealed that employees' involvement can be seen as supportive and as an enabler for compliance. According to Fathi *et al.* (2011), employees' involvement generates a suitable atmosphere through lines of communication and knowledge sharing. Furthermore, Reagan and Mcevily (2015) argue that employees' involvement contributes to the creation and maintenance of policies.

4.4.3 Information systems as Facilities

The use of technology includes hardware and software, as the facilities on which human actors draw. According to Lyytinen and Ngwenyama (1992), facilities are either material or non-material resources, which enable actors to use power over social action to interact with it. As such, facilities enable actors to draw on and reproduce structures of domination. The actors' interaction includes both social and system. According to Giddens (1984), social interaction is a process of reciprocity that includes autonomy and dependency between actors which involves social practices such as self-service technology. System interaction includes reciprocity between actors across an extended time space, as all social interactions are situated in time and space. Facilities are becoming part of a person's life; they can be understood as a routine that occurs in time and space

that require regular features of encounters, and represent institutionalised features of social systems. Individual actions are neither determined by technology, nor are they constructed by technology concepts.

The DoT is explored to understand the relationship between technologies and human actors in order to ensure security of information. Individual actions are determined neither by technology nor by lack of knowledge about technology. The technology itself cannot provide security of information; thus, the combination of human beings and technology is a key factor to prevent security issues. Through the use of technology, several benefits including fast access to information, knowledge sharing, communication, education, and integration contribute significantly for employees to engage with compliance. This indicates that employees, through the use of power exercise through technology dominates with the view to enact and sustain better human management and resource allocation.

The literature review suggested that technology would drive policies needed in order to enforce compliance. The outcomes revealed that technology enables the institution to access information faster. This means that the use of technology facilitates communication, transaction and knowledge sharing amongst employees across the institution. These were affirmed by bellow comments made by a VU secretary:

Technology indeed can provide fast access to information, needed [for] training purposes....using technology enables communication and knowledge sharing amongst employees.

Similarly, an assistant manager from VU added:

Technology brings many benefits such as creating and maintaining social networking amongst employees, online management support, etc.

Finally, a CPUT manager added:

Technology involves policies or instructions... those instructions have to be complied with. For me, technology means creating,

learning, instructing, applying and complying with the instructions.

The findings revealed that technology is considered to be useful, in general, while not as much for some. Other respondents perceived that technology brought fraud, corruption, theft and other online bad behaviours. This was confirmed by a CPUT manager:

Technology brings online robbery, fraud... and our children are learning bad behaviours from certain online websites.

Despite these findings, the majority of respondents were in positive agreement with the idea that technology plays a significant role in supporting compliance. Technology is used as a medium and product of human action. It refers to the facilities, resources, instruments, tools or materials that facilitate the usability and execution of tasks. Resources are the tools or instruments designed and reproduced by human agents during the course of an interaction; these resources facilitate the execution of tasks. Furthermore, Orlikowski and Baroudi (2000) stated that technology is an outcome of human action through innovation, concept, modification and process. The research outcomes revealed that employees can share their knowledge by using technology. As such, technology can be used to enable lines of communication, culture, policies and the participation and coordination of different departments, thereby providing instructions through which the process of compliance can take place.

Technology works when instructions and policies are in place, in order to be used correctly; thus, employees need to comply with policies given for the better use of technologies and the compliance thereof. Drawing from the DoT, the construct norms are a set of rules or policies established in order to protect information and technology resources. The norms are the rules that are imposed on employees in order to be complied with. Employees or actors draw on norms - such as policies - that inform their ongoing practices.

Studies of the use of technology have found that interpretive scheme shapes how employees interact with technologies within their work. According to Yoshioka *et al.* (2002), the influence of interpretive schemes arises because employees have to make sense of technology in order to engage with it. In this sense, when making a process, employees can draw on their existing policies, beliefs and knowledge about the technology and what counts as the proper use of it within

their institutions. In this way, interpretive schemes serve to structure employees' understandings of - and interaction with - technology.

According to Mauerer and Nissen (2014), Facility can be appropriated through the domination, which exerts power that comes from controlling of resources. As such, Gao (2007) stated that human agents utilise power upon facilities, including the ability to distribute human resources. According to Giddens (1984), domination includes the control and use of allocative and authoritative resources, alongside with power over people or resources. The outcomes revealed that the use of technology drives the implementation of policies. Thus, it involves controlling and using facilities laterally with compliance.

4.4.4 Information Security Policies as Norm

Policies are used as a set of rules and guidelines - established by institutions - to address particular security issues by clarifying the need for IS. In other words, policies are a set of documentation of enterprise-wide decisions on how to handle and protect information. They are part of the institution's integral objectives. They are needed in institutions for the safety of both private and institutional information. Therefore, employees have to comply with their existing policies in order to protect information from security breaches.

Institutions establish policies as rules and instructions to guide employees and secure information through compliance. As such, they increase employees' performance, knowledge and the skills needed. This study mentioned that the increase of knowledge is justified by many factors, including communication of the policies, awareness, training, education, leadership skills and motivation and support from management. In the context of this study, policies must be clear, well defined and understandable. They must indicate the institution's attitude towards compliance and claim the "information" as the property of the institution.

To have policies in place constitutes a significant enabler that can set an employees' mind on how to share knowledge. Conversely, having InfoSecPols in place does not guarantee compliance. The assumption is that InfoSecPols implementation alone does not influence employees' compliance. Therefore, considering that a policy in itself cannot induce employees to comply, standard operating procedures have been identified as a mechanism that can efficiently influence and enforce compliance defining - and driving - how the share of knowledge would occur in lines of communication.

It was suggested that structural management can be an effective enabler for compliance with InfoSecPols. It was revealed in the research that structural management empowers and drives compliance. According to the data that was analysed, structural management is an important factor that enables compliance. The outcomes presented different techniques in which structural management must be implemented for enforcing compliance with InfoSecPols. A VU manager commented as follows:

Management structure is an important enabler for compliance with InfoSecPols in terms of knowledge sharing...

Similarly, a VU assistance manager made this statement:

A good management structure promotes compliance with InfoSecPols through communication...Management motivates and influences employees to comply effectively with policies.

Based on the above statements, it is evident that structural management influences knowledge sharing through the lines of communication. As such, management imposes the policies through the institutional structure. As an enabler, structural management is a technique of using power by creating a body which manages standard operating procedures. Nevertheless, structural management creates a dual reporting line between managers and employees. It enforces communication, motivates compliance and encourage employees to share knowledge.

As a CPUT manager stated:

A management structure empowers managers to implement and enforce compliance. This means that we are part of the corporate services directorate that implement policies and enforce[s] them in the institution. We have the power to create policies and impose them through compliance.

The outcomes affirmed that structural management establishes a relationship between managers and employees, through lines of communication. As such, managers create policies and then share the knowledge amongst employees. Additionally, this points toward the relationship that must take place for employees to comply. Given that management set strategies that must be implemented in discussion with employees, structural management provides the basis for lines of communication and knowledge sharing amongst employees.

The outcomes of the research revealed that structural management enables drive - and provides directives from top management and ordinary staff - on what type of and how knowledge must be shared, in the organisation. According to Sharratt and Usoro (2003), structural management influences the lines of communication and knowledge sharing. The communication and knowledge sharing must be driven by top managers in order to influence compliance with policies. Furthermore, Frost (2014) stated that structural management influences awareness and positively motivates employees to engage with knowledge sharing through lines of communication. Therefore, the findings are in agreement with that of the literature; the findings revealed that structural management ensures compliance with InfoSecPol.

4.4.5 Conclusion

Given the concept of dimension of DoT/structure as a lens, the phenomenon of the perception of employees concerning InfoSecPol (based on case studies of a European and a South African university) was understood and interpreted. The outcome of this study showed that compliance with policies was achieved through the institutionalisation of InfoSecPol, and that it can be reproduced through structural management, implementation, controlling and evaluation of these approaches, from which recommendations are designed to make them more operative.

4.5 PROPOSED GENERAL FRAMEWORK

Figure 4.1 presents a proposed general framework, as a revision of the problem conceptualisation based on the results of the findings from the qualitative data analysis (as discussed above). This proposed general framework demonstrates structural management, through the enactment of compliance with policies in practices.

In the context of this study, insights were obtained from elements found in literature and the answers to the interview questions. As stated in the problem statement, information is considered

to be the most valuable asset of institutions. For that reason, institutions are totally reliant on information for their sustainability, functionalities and competitiveness. Institutions, therefore, ensure that information about their processes, activities and services are secured, which they do through enforcement and compliance with policies.

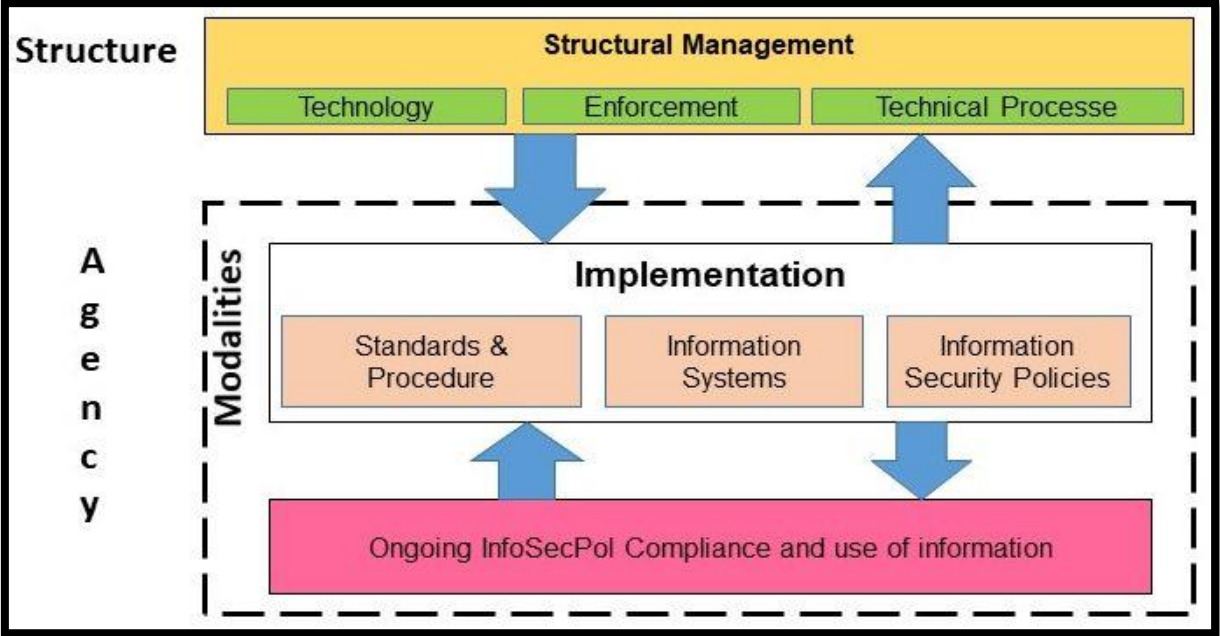


Figure 4.1: Proposed General Framework

In the general framework introduced above, the structural management involves compliance with policies in practice, through the use of interpretive schemes such as InfoSecPols, Norms as appropriate practice and governance, and technology as Facilities. These modalities created the mode of interaction, which are the lines of communication for implementation made possible through an employee’s involvement, standards and procedures, and information systems through a normative set of InfoSecPols. In this context, there is a power, which involves the ability of employees to take control of resources, which involves the use of technology, leading to compliance with policies. As such, the relationship between the modalities and the modes of interaction contribute to the production of the structural management in practice, thereby confirming the use of the concept of duality of structure.

4.6 SUMMARY

This Chapter presented the results and interpretation of the findings generated from the qualitative approach. The data was analysed using content analysis. Founded on the underpinning concept

of the duality of structure, major components of the theory of structuration were used as a theoretical lens through which the research questions were addressed and answered. The outcomes indicated that the institutionalisation of InfoSecPols are reliant on the operational enactment of compliance in practice, through interpretive schemes which involve people, policies, technology and standard operating procedures. In addition, these schemes also included norms (which are the values and practices) motivated by an adequate governance process, organisational culture and support from the management.

The factors of facilities have been presented as the use of technology, endorsed through the implementation of information systems, technical processes, technology and enforcement. In this case, the compliance with InfoSecPols is effective.

CHAPTER FIVE: CONCLUSION AND RECOMMENDATION

5.1 INTRODUCTION

In the previous Chapter, the analysis and the interpretation of the findings obtained from interviews were presented. The duality of structure concept guided the findings as a theoretical lens through which the entire research was conducted. This is due to the fact that this study aimed to explore the extent of non-compliance with InfoSecPols. The aims and objectives of this study were achieved through the use of a multiple-case study. The semi-structured interviews and documents, including websites from the selected case studies, were the sources of data collection. The participants were selected based on criteria such as their positions, roles and responsibilities assumed within the departments. This included HR managers, administrative managers, assistant managers and secretaries, who all provided good insights. Content analysis was used to analyse the data obtained from the qualitative approach. The data obtained from the responses was analysed. The duality of structure/technology concept served to categorise the themes identified and to interpret the findings.

This Chapter discusses the research objectives, contribution, limitations, recommendation and future research studies. Finally, the Chapter concludes the research study.

5.2 OVERVIEW OF THE RESEARCH

The aim of this research study was to explore the extent of non-compliance within an institution's InfoSecPol. Based on this aim, the main objective was to investigate the extent to which non-compliance of InfoSecPols by employees in an institution would affect its functioning, growth and sustainability. The sub-objectives, therefore, were:

- i) To determine how InfoSecPols are enforced in an institution;
- ii) To investigate the factors that influence non-compliance of the InfoSecPols in an institution;
and
- iii) To determine the factors that influence compliance of the InfoSecPols in an institution.

The objectives of this study were achieved using the concept of duality of structure. This led to the proposed framework as a revision of the problem conceptualisation, based on the results of the findings from the qualitative data analysis (as discussed above).

In Chapter one, the introduction to the research and the background to the research problem were presented. This was followed by a problem statement, research questions, aims and objectives of the research, contribution of the research, research limitation and ethical considerations of the study.

Chapter Two provided an in-depth literature review, which included past scientific research by known scholars and authorities in InfoSecPol, and the various phenomena that have been investigated. The Chapter ended with explanations of the proposed theory on IS, which used ST as a lens to view and interpret the data.

Chapter Three covered the research approaches and methodologies. It provided an overview of the philosophical assumptions, paradigms and research approach. It also described the data collection methods and analysis strategies used. The validation and ethical considerations were also discussed.

Chapter Four presented the theory used as a lens to view and interpret the data. The Chapter also presented the analytical process that was followed, to analyse the data from the interviews, and provided answers to the research questions.

Chapter Five discussed the research objectives, contribution, limitations, recommendation and future research studies. Finally, the chapter concluded the research study.

The next section discusses the findings that emerged from the sub-research questions. Additionally, the theoretical and practical implication and contribution of this research study will be also discussed. Finally, the section will discuss the research limitations and recommendations for future research.

5.3 ENFORCEMENT OF INFORMATION SECURITY POLICIES

As discussed in sections above, the use of policies, human involvement, standard operating procedures, organisational culture, education, knowledge sharing, social engagement, lines of communication, management support and technology can enforce IS policies. These factors enable adequate policy alignment and enforcement. In addition, mandated policies can enforce the type of normative sets of rules needed for compliance. This means that a mandate is an authorised method of acting in different ways. Given the above factors that enable the enforcement

of InfoSecPols, it indicates that having policies in place does not guarantee enforcement. As such, standard operating procedures have been identified as a mechanism that can efficiently influence and enforce compliance with policies by defining and driving how the share of knowledge would occur in lines of communication.

Additionally, organisational structure has been identified as an important factor for enforcing InfoSecPols in an institution. The findings revealed that this requires a body, driven by managers, that can focus on the issue of knowledge management and knowledge sharing in the institution. The body of management has the particularity to enable, drive and provide strategic directive, from top managers to ordinary staff, on what type of and how knowledge can be shared. Furthermore, the findings revealed that employees' involvement need to be considered because - without human capital - the share of knowledge and enforcement of InfoSecPols would not occur. In the context of this study, employees are considered as central for the success of education, knowledge sharing and enforcement of an InfoSecPol in an organisation. They are the medium through which knowledge and other features occur. This means that, without employees' involvement, policies and standard operating procedures or organisational structures would not exist; these are the demonstrations brought by human involvement. Also, the findings revealed that the use of technology/information systems enforces an InfoSecPol in the way that it enables the increase of knowledge, performance, guidance and learning processes, thereby improving the line of communication to enforce compliance with policies.

Finally, governance was also identified as an important type of normative sets of values that enhance the enforcement of an InfoSecPol. In the context of this study, governance enforces best practices that involves knowledge management strategies. It was predicted that governance can enforce the normative set of rules needed for the enforcement of an InfoSecPol, which leads to compliance.

5.4 FACTORS OF NON-COMPLIANCE OF INFORMATION SECURITY POLICIES

The findings of this study revealed some factors that influence non-compliance with InfoSecPols, including a lack of awareness, training, education, misuse and abuse of facilities, insufficiency of resources, fraud, theft, corruption and lack of transparency, lack of leadership skills, poor implementation of sets of norms and values, a lack of incentive structures and inexperienced staff members, amongst others. The outcomes revealed that institutions are facing challenges of a different nature, including a low level of education, an inadequate social environment and the lack

of social norms. Some of the challenges are due to the lack of knowledge about Information Security Policies, insufficiency of resources and lack of management support.

Given the responses above, it is agreeable that standard operating procedure and Norms are required to drive moral codes and values for policy compliance. However, the findings also revealed that factors which influence non-compliance with policies are not qualified to be part of duality of structure. This is because the modalities of structure such as interpretive schemes, norms and facilities are not applied appropriately or used as required by the duality of structure. Moreover, the findings revealed that the factors of non-compliance with InfoSecPols have serious consequences to an institution, including an inability to:

- i) sustain institutional goals and objectives;
- ii) carry out the service effectively and efficiently;
- iii) compete in the industry or market; and
- iv) manage the activities of the institution.

Thus, these consequences sometimes led to job losses or an institution's closure.

5.5 FACTORS OF COMPLIANCE FOR INFORMATION SECURITY POLICIES

In the context of this study, the main factors of norms that influence compliance with information security policies include governance, standard operating procedures, education, awareness, leadership skills, technology, organisational structures, management support, mandate, performance management and knowledge sharing. The findings revealed that these factors enable proper policy alignment for the improvement of compliance with InfoSecPols.

Given the responses above, it is argued that the factors influencing compliance of policies (such as the support from the management) enables dual reporting lines between managers and employees. In light of this, management support enables managers to drive and implement the type of moral codes and beliefs needed to make lines of communication more effective. Moreover, these factors of policy compliance influence and motivate employees to engage more with knowledge. Also, the findings revealed that performance management can assist to enforce the normative set of rules needed for an effective compliance.

Furthermore, the outcomes revealed that organisational culture is an important factor that influences compliance with policies. It is evident that organisational culture drives the norms needed for knowledge sharing in the institution.

Moreover, the findings revealed that the factors that influence compliance with an InfoSecPol increases an employee's performance, knowledge and skills needed, including the ability to:

- i) sustain institutional goals and objectives;
- ii) carry out the service effectively and efficiently;
- iii) compete in the industry or market; and
- iv) manage the activities of the institution.

5.6 RESEARCH CONTRIBUTIONS

5.6.1 Methodological Contribution

The qualitative approach and research expanded the information provided for this study, as it included the relevant perception of the participants, their understandings, opinions, explanations and experiences based on the field of study. The qualitative research methods focused on the qualities of the subjective experience of the employees and their meanings associated with the phenomena. Additionally, the study drew from the interpretivist paradigm of the epistemological philosophy and was founded on case studies from two institutions, one in Cape Town and another in The Netherlands, as the units of analysis.

The findings generated from the qualitative perspective enhances the reliability and the validity of the research findings, where richness of the information obtained brought so much meaning for a solution to the phenomenon. Additional methodological contribution is the type of data analysis methods followed in this study. Content analysis was used to analyse the data generated from the qualitative approach. This allowed for the collection of in-depth data through content analysis.

5.6.2 Theoretical Contribution

This theoretical contribution comes from the application of the underpinning theory, which is based on the dimensions of DoT of ST. The research questions, data collection instrument and analysis were guided by this theory. The theory was used as a lens to understand and conceptualise the problem and to derive the research questions as:

- i) Determining how InfoSecPols are enforced in an institution;
 - ii) Investigating the factors that influence non-compliance with InfoSecPols in an institution;
- and

- iii) Determining the factors that influence compliance with InfoSecPols in an institution.

Furthermore, the application of the concept of DoT/structure as a theoretical lens through which this research study was conducted justifies the adoption of qualitative approach. The relationship between structure and agency - and the interactions thereof - was understood better, if not the use of the DoT/structure as a lens that led to the proposal of a general framework.

5.6.3 Practical Contribution

The practical contribution of this study extends to the understanding of issues of the extent of non-compliance within an organisation's InfoSecPol, over an interpretive case study methodology. Practitioners may use the proposed general framework to explore the extent of non-compliance of IS policies in an organisation. They will have clear ideas of the types of security knowledge, management strategies, and the procedures to follow for improvement. Therefore, management and employees will be able to direct and manage the extent of non-compliance with policies. Routine use and compliance will institutionalise InfoSecPols in the organisation.

5.7 RESEARCH LIMITATIONS

This research study was limited to two departments from the two institutions, namely the HR Department and the Administrative office, including 17 participants (including HR managers, administrative managers, assistant managers and secretaries, working in the selected departments). The study focused on exploring the extent of non-compliance on InfoSecPols in two institutions, one from Amsterdam in The Netherlands and another from Cape Town in South Africa. It would have benefitted this study to have included more institutions and participants from other departments.

5.8 CONCLUSION AND RECOMMENDATION AND FUTURE RESEARCH

This study discussed the factors that influence compliance with policies, the factors of non-compliance with policies and determined how an InfoSecPol is enforced in an institution. Furthermore, the study discussed how non-compliance with IS policies by employees in an institution can be managed. It was therefore important to address and understand the extent of non-compliance with policies. The dimension of DoT and ST was used as a lens to understand and interpret the research problem. This theory enabled the conceptualisation of the problem and,

with the analysis and interpretation of the data collected, revised the framework to a general framework. The findings confirmed that on-going use and compliance of an InfoSecPol is enhanced by structural management through the technology and culture of compliance. This is in terms of knowledge sharing, knowledge management strategies and governance, which enforce, influence, monitor and evaluate the process for compliance with InfoSecPols.

This research made use of the duality of structure/technology of ST as a lens through which the extent of non-compliance with policies was identified. This study recommends that other researchers use different social theories to determine whether similar factors would emerge from the research findings.

REFERENCES

- Abou-Zeid, E.-S. 2007. A Theory-Based Approach to the Relationship between Social Capital and Communities of Practice. *Electronic Journal of Knowledge Management*, 5(3): 257–264.
- Accorsi, R., Lehmann, A. & Lohmann, N. 2015. Information leak detection in business process models: Theory, application, and tool support. *Information Systems*, 47, 244-257.
- Ajzen, I. 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(1): 179–211.
- Al-Shbiel, S. O. & Ahmad, M. A. 2016. A theoretical discussion of electronic banking in Jordan by integrating technology acceptance model and theory of planned behavior. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, 6(3): 272-284.
- Alvesson, M. 2003. Beyond neopositivists, romantics, and localists: A reflexive approach to interviews in organizational research. *Academy of Management Review*, 28(1), 3-33.
- Babbie, E. & Mouton, J. 2011. The practice of social research South African edition. *Oxford University press Southern Africa* (pty) Ltd.: 150-265.
- Babbie, E. 2013. The practice of social research. 13th ed. Belmont: Wadsworth, Cengage Learning.
- Baxter, P. & Jack, S. 2008. Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report*, 13(4): 544-559. Retrieved from <http://nsuworks.nova.edu/tqr/vol13/iss4/2>
- Bayrak, T. 2012. IT Support Services for telecommuting workforce. *Telematics and Informatics*, 29(3):286-293.
- Bhattacharjee, A. 2012. Social science research: principles, methods and practices. 2nd ed. Florida: Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.
- Boss, S., Galletta, D., Lowry, P.B., Moody, G.D. & Polak, P. 2015. What Do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly (MISQ)*, 39 (4): 837-864.
- Braun, V. & Clarke, V. 2013. Successful qualitative research: A practical guide for beginners. Sage.
- Brown, P., Beekes, W. & Verhoeven, P. 2011. Corporate governance, accounting and finance: A review. *Accounting & finance*, 51(1): 96-172.

- Bulgurcu, B., Cavusoglu, H. & Benbasat, I. 2010. (InfoSecPol) compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3): 523-548.
- Babu, B.R. & Gopalakrishnan, S., 2008. Knowledge Sharing Tools and Technology: An Overview. *Journal of Library & Information Technology*, 28(5): 19–26.
- Burke, L.A. & Miller, M.K. 2001. Phone interviewing as a means of data collection: lessons learned and practical recommendations. *Forum: Qualitative Social Research*, 2(2):1-8.
- Cavaye, A. L. M. 1996. Case Study Research: A Multi-Faceted Research Approach For IS. *Information Systems Journal*, 6(3), 227-242.
- Chen, H. & Li, W. 2014. Understanding organisation employee's information security omission behaviour: an integrated model of social norm and deterrence. In the Proceedings of Pacific Asian Conference on Information Systems (PACIS). Chengdu, China.
- Chen, Y. & Özer, Ö. 2017. Supply Chain Contracts that Prevent Information Leakage. Available at SSRN: <https://ssrn.com/abstract=2728017> or <http://dx.doi.org/10.2139/ssrn.2728017>. Accessed on 16 July 2017.
- Chang, C.L.H., 2014. The interaction of political behaviors in information systems implementation processes - Structuration Theory. *Computers in Human Behavior*, 33,79–91.
- Chen, Y., Ramamurthy, K. & Wen, K. W. 2012. Organizations' (InfoSecPol) compliance: Stick or carrot approach?. *Journal of Management Information Systems*, 29(3): 157-188.
- Chisita, C.T. & Chinyemba, C. 2017. Utilising ICTs for Resource Sharing Initiatives in Academic Institutions in Zimbabwe: Towards a New Trajectory. In *Managing Knowledge and Scholarly Assets in Academic Libraries*. IGI Global book series Advances in Library and Information Science, USA.
- Choi, K.H. & Lee, D. 2015. A study on strengthening security awareness programs based on an RFID access control system for inside information leakage prevention. *Multimedia Tools and Applications*, 74 (20): 8927-8937.
- Chris, L. A. 2015. Barriers Hindering Implementation, Innovation and Adoption of ICT in Primary Schools in Kenya. **International Journal of Innovative Research and Development**, 4(2): 1-7. Available at: <http://www.ijird.com/index.php/ijird/article/view/60046> Date accessed: 12 Feb. 2016.
- Colwill, C. 2010. Human factors in information security: The insider threat–Who can you trust these days? Information security technical report, 14(4): 186-196.
- CPUT, 2015. Available at www.cput.ac.za/about/visit/cape-town-campus, accessed on 20 April 2016.
- Creswell, J. W. (2009). Research design: Qualitative, quantitative, and mixed methods approaches. Thousand Oaks, Calif.: Sage.

- Creswell, J.W. 2009. Research design: Qualitative, quantitative and mixed approaches. 3rd ed. California: SAGE Publications, Inc.
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. & Baskerville, R. 2013. Future directions for behavioral information security research. *Computers & Security*, 32, 90-101.
- Da Veiga, A. & Martins, N. 2015. Improving the information security culture through monitoring and implementation actions illustrated through a case study, *Computers & Security*, 49,162-176.
- Dao, V., Langella, I. & Carbo, J. 2011. From green to sustainability: Information Technology and an integrated sustainability framework. *The Journal of Strategic Information Systems*, 20(1):63-79.
- Desourdis, R. I., Collins, K. H. & Rosamilia, P. J. 2016. Human collaboration in Homeland security: Collaboration planning for day-to-day and hastily formed networks. In *Technologies for Homeland Security (HST), 2016 IEEE Symposium* , 1-8. IEEE.
- Doane, A. N., Boothe, L. G., Pearson, M. R. & Kelley, M. L. 2016. Risky electronic communication behaviors and cyberbullying victimization: An application of Protection Motivation Theory. *Computers in Human Behavior*, 60, 508-513.
- Du Plooy-Cilliers, F. & Cronje, J. 2014. Research paradigms and traditions. Research Matters. Cape Town: Juta.
- Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, 14(4), 532:550.
- Elbasha, T. & Wright, A. 2017. Reconciling structure and agency in strategy -as-practice research: Towards a strong-structuration theory approach, *Management*, 20(2): 107-128.
- Elhai, J. D. & Hall, B. J. 2016. Anxiety about internet hacking: Results from a community sample. *Computers in Human Behavior*, 54, 180-185.
- Esch, E.V., Wei, L.Q. & Chiang, F.F.T. 2016. High-performance human resource practices and firm performance: the mediating role of employees' competencies and the moderating role of climate for creativity. *The International Journal of Human Resource Management*, 1(1): 1-26.
- Farahmand, F. & Spafford, E. H. 2013. Understanding insiders: An analysis of risk-taking behavior. *Information systems frontiers*, 15 (1): 5-15.
- Fouché, C. & Delpont, C. 2011. Introduction to the research process. In De Vos, A.S., Strydom, H., Fouché, C.B. & Delpont, C.S.L. (eds). *Research at grass roots, for the social sciences and human service professions*. Pretoria: Van Schaik: 61-76.
- Frost, A. 2014. A synthesis of knowledge management failure factors. Retrieved January, 5, 2015.

- Frishammar, J., Ericsson, K. & Patel, P. C. 2015. The dark side of knowledge transfer: Exploring knowledge leakage in joint R&D projects. *Technovation*, 41, 75-88.
- Furnell, S.N., Von Solms, V.R. & Safa, S.N. 2016. (InfoSecPol) compliance model in organizations. *Computers & Security*, 56(16):70-82.
- Giddens, A. 1984. *The Constitution of Society*, Cambridge: Polity Press.
- Gravetter, F.J. & Forzano, L-A. B. 2009. *Research Methods for the Behavioral Sciences* (3rd ed.). Belmont, CA: Wadsworth.
- Greenaway, K. H., Wright, R. G., Willingham, J., Reynolds, K. J., & Haslam, S. A. 2015. Shared identity is key to effective communication. *Personality and Social Psychology Bulletin*, 41(2): 171-182.
- Hashim, J. 2015. Information Communication Technology (ICT) Adoption among SME Owners in Malaysia. **International Journal of Business and Information**, 2(2):221-227. Available at: <http://ijbi.org/ijbi/article/view/20>. Date accessed: 12.March 2017.
- Hedström, K., Karlsson, F.& Kolkowska, E. 2013. Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale. *Information Management & Computer Security*, 21(4): 266-287.
- Herath, T. & Rao, H. 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2): 106-125.
- Huang, M.-C., Chiu, Y.-P. & Lu, T.-C. 2013. Knowledge governance mechanisms and repatriate's knowledge sharing: the mediating roles of motivation and opportunity. *Journal of Knowledge Management*, 17(5): 677–694.
- Høstland, K., Enstad, P. A., Eilertsen, Ø. & Bøe, G. 2010. (InfoSecPol). Norway.
- Hycner, R. H. (1985). Some guidelines for the phenomenological analysis of interview data. *Human Studies*, 8(3), 279–303.
- Ifinedo, P. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1):83-95.
- Ifinedo, P. 2014. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, 51(1):69-79.
- Jafarkarimi, H., Saadatdoost, R., Simc, A.T.H. & Hee, J.M. 2016. Behavioral intention in social networking sites ethical dilemmas: An extended model based on Theory of Planned Behavior. *Computers in Human Behavior*, 62 (16): 545–561.
- Jansen, J. 2010. Strategic information disclosure and competition for an imperfectly protected innovation. *The Journal of Industrial Economics*, 58(2): 349-372.
- Ju Choi, C. et al., 2010. Knowledge governance. *Journal of Knowledge Management*, 9(6):67–75.

- Jonsson, A. & Kalling, T., 2007. Challenges to knowledge sharing across national and intra-organizational boundaries: case studies of IKEA and SCA Packaging. *Knowledge Management Research; Practice*, 5(3): 161–172.
- Jones, M. & Karsten, H., 2003a. Review: Structuration Theory and Information Systems Research. *Management*, 32, 25–33.
- Jiang, X., Li, M., Gao, S., Bao, Y. & Jiang, F. 2013. Managing knowledge leakage in strategic alliances: The effects of trust and formal contracts. *Industrial Marketing Management*, 42(6): 983-991.
- Johnston, A., Warkentin, M., McBride, M. & Carter, L. 2016. Dispositional and situational factors: influences on (InfoSecPol) violations. *European Journal of Information Systems*, 25(3): 231–251.
- Karjalainen, M. & Siponen, M. 2011. Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, 12(8): 518-555.
- Katos, V. & Adams, C. 2005. Modelling corporate wireless security and privacy. *The Journal of Strategic Information Systems*, 14(3): 307-321.
- Kayombo, J.J. & Mlyakado, B.P. 2015. The paradox of ICT integration in secondary education in Tanzania: Assessment of teachers' ICT knowledge and skills in Tanga and Mwanza regions, *International Journal of Research Studies in Educational Technology*, 5(1): 17-27.
- Kearney, W. D. & Kruger, H. A. 2016. Can perceptual differences account for enigmatic information security behaviour in an organisation?. *Computers & Security*, 61, 46-58.
- Kearney, W. D. & Kruger, H. A. 2016. Can perceptual differences account for enigmatic information security behaviour in an organisation?. *computers & security*, 61, 46-58.
- Kessy, D., Kaemba, M. & Gachoka, M. 2006. The reasons for under use of ICT in education: in the context of Kenya, Tanzania and Zambia, Fourth IEEE International Workshop on Technology for Education in Developing Countries (TEDC'06), Iringa, 83-87.
- Kolkowska, E., Karlsson, F & Hedström, K. 2017. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. *The Journal of Strategic Information Systems*, 26(1): 39-57.
- Kotlar, J. & Massis, A. D. 2014. The case study method in family business research: Guidelines for qualitative scholarship. *Journal of Family Business Strategy*, 5(1): 15-29.
- Kramers, A., Höjer, M., Lövehagen, N., Wangel, J. 2014. Smart sustainable cities: exploring ICT solutions for reduced energy use in cities. *Environ. Model Softw.* **56**, 52–62.
- Leitch, S. & Warren, M. 2009. Security issues challenging Facebook. Paper presented at the 7th Australian Information Security Management Conference, Perth, Western Australia, 137-141.

- Loenen, V.J. 2015. Information security awareness. *Research world*, 54 (15):53.
- Lin, H.-F.H.-F., 2007. Knowledge sharing and firm innovation capability: an empirical study. *International Journal of Manpower*, 28(3/4), 315–332.
- Luo, Y. & Bu, J. 2016. How valuable is information and communication technology? A study of emerging enterprises. *Journal of World Business*, 51(2):200-211.
- Larsson, A.O., 2012. Understanding Nonuse of Interactivity in Online Newspapers: Insights From Structuration Theory. *The Information Society*, 28(4), pp.253–263.
- Madlock, P.E. 2012. The influence of supervisors' leadership style on telecommuters. *Journal of Business Strategies*, 29(1):1-24.
- Mauerer, C. & Nissen, V., 2014. Portraying the social dimensions of consulting with structuration theory. *Journal of Services Science and Management*, 7(April), 110– 130.
- Madlock, P.E. 2013. The influence of motivational language in the technologically mediated realm of telecommuters. *Human Resource Management Journal*, 23(2):196-210.
- Madlock, P.E. 2013. The influence of motivational language in the technologically mediated realm of telecommuters. *Human Resource Management Journal*, 23(2):196-210.
- Merriam, S. B. (2009). *Qualitative research: A guide to design and implementation* (2nd ed.). San Francisco, CA: Jossey-Bass.
- Muljono, W. 2017. Technological Determinism in Patterns of Communication and Social Behavior Change in Indonesian Society. *Asian social science*, 13(2): 12.
- Myers, M.D. 1997. Qualitative research in Information Systems. *MIS Quarterly*, 21(2):1-8.
- Neuman, L.W. 2011. *Social research methods: qualitative and quantitative approaches*. 6th ed. Boston: Pearson Educational, Inc.
- Nord, J.H., Riggio, M.T. & Paliszkiwicz, J. 2017. Social and Economic Development through Information and Communications Technologies: Italy. *Journal of computer information systems*, 57(3): 278-285.
- Nyaanga, S.G. 2012. The Impact of Telecommuting Intensity on Employee Perception Outcomes: Job Satisfaction, Productivity and Organizational Commitment. *ProQuest LLC*, Ph.D. Dissertation, Stevens Institute of Technology. Available at <http://www.proquest.com/en-US/products/dissertations/individuals.shtml>. Accessed on 15 March 2017.
- Orlikowski, W.J. & Baroudi, J.J. 1992. Studying Information Technology in organizations: Research approaches and assumptions. *Information Systems Research*, 2(1):1-28.
- Orlikowski, W.J. & Robey, D., 1991. Information Technology and the Structuring of Organisations. *Information Systems Research*, 2(2), pp.143–169.

- Palacios-Marqués, D., Soto-Acosta, P. & Merigó, J.M. 2015. Analyzing the effects of technological, organizational and competition factors on Web knowledge exchange in SMEs. *Telematics and Informatics*, 32(1):23-32.
- Pham, H.T. & Tanner, K., 2015. Australian Academic & Research Libraries Collaboration Between Academics and Library Staff: A Structurationist Perspective. *Australian Academic & Research Libraries*, 46(January), pp.37–41.
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. & Jerram, C. 2014. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security*, 42,165-176.
- Pinsonneault, A. & Pozzebon, M., 2001. Structuration Theory in the IS Field: An Assessment of Research Strategies. In *Information Systems*. 205–217
- Patton, M. Q. 2002. *Qualitative evaluation and research methods* (3rd ed.). Newbury Park, Calif.: Sage.
- Pietkiewicz, I. & Smith, J. A. 2012. A practical guide to interpretive phenomenological analysis in qualitative research in psychology. *Psychological journal*, 18(2):361-369.
- Ponelis, S. R. 2015. Using interpretive qualitative case studies for exploratory research in doctoral studies: A case of Information Systems research in small and medium enterprises. *International Journal of Doctoral Studies*, 10, 535-550. Retrieved from <http://ijds.org/Volume10/IJDSv10p535-550Ponelis0624.pdf>
- Rees, G. & Smith, P.E. 2014. *The organisation: the organisational context and strategy*. Strategic Human Resource Management. India: Sage.
- Rose, J. & Scheepers, R. 2001. Structuration theory and information system development-frameworks for practice. *ECIS 2001 Proceedings*, 80, 1-17.
- Ryan, G.W. & Bernard, H.R. 2003. Techniques to identify themes. *Field Methods*, 15(1):85-109
- 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 & Security*, 53, 65-78.
- Safa, N.S. & Von Solms, R. 2016. An information security knowledge sharing model in organizations. *Computers in Human Behavior*, 57,442-451.
- Shorunke, O.A.A. et al., 2014. Organisational Support, Knowledge Sharing and Utilisation as Correlates of Social Capital of Insurance Managers in Lagos Metropolis. *Information and Knowledge Management*, 4(8): 53–64.
- Saldana, J. 2009. *The coding manual for qualitative researchers*. London: Sage.

- Saridakis, G., Benson, V., Ezingard, J.N. & Tennakoon, H. 2016. Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, 102, 320-330.
- Sharratt, M. & Usoro, A., 2003. Understanding Knowledge-Sharing in Online Communities of Practice. *Electronic Journal on Knowledge Management*, 1(2):187–196.
- Saunders, M., Lewis, P. & Thornhill, A. 2009. *Research Methods for Business Students*. Harlow, England, UK: Pearson Education Limited.
- Shaw, E. 1999. A guide to the qualitative research process: Evidence from a small firm study. *Qualitative Market Research: An International Journal*, 2(2), 59–70.
- Shih, H. P., Guo, X., Lai, K. H. & Cheng, T. C. E. 2016. Taking promotion and prevention mechanisms matter for information systems security policy in Chinese SMEs. In *Information Management (ICIM), 2016 2nd International Conference* , 110-115. IEEE.
- Siponen, M., Mahmood, M. A. & Pahnala, S. 2014. Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2): 217-224.
- Sommestad, T., Hallberg, J., Lundholm, K. & Bengtsson, J. 2014. Variables influencing (InfoSecPol) compliance: a systematic review of quantitative studies. *Information Management & Computer Security*, 22(1): 42-75.
- Soomro, Z.A., Shah, M.H. & Ahmed, J. 2016. Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2): 215-225.
- Soto-Acosta, P., Placer-Maruri, E. & Perez-Gonzalez, D. 2016. A case analysis of a product lifecycle information management framework for SMEs. *International Journal of Information Management*, 36(2): 240-244.
- Soto-Acosta, P., Popa, S. & Palacios-Marqués, D. 2015. E-business, organizational innovation and firm performance in manufacturing SMEs: an empirical study in Spain. *Technological and Economic Development of Economy*, 22(6): 885-904.
- Stahl, B. C., Doherty, N. F. & Shaw, M. 2012. Information security policies in the UK healthcare sector: a critical evaluation. *Information Systems Journal*, 22(1): 77-94.
- Stake, R. E. 2005. Qualitative case studies. In N. K. Denzin & Y. S. Lincoln (Eds.), *The Sage handbook of qualitative research* (3rd ed.) (pp. 443-466). Thousand Oaks, CA: Sage
- Stones, R. 2014. Social theory and current affairs: a framework for intellectual engagement. *British Journal of Sociology*. 65(2): 293-316.
- Strauss, A., & Corbin, J. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Thousand Oaks, CA: Sage.

- Susanne, D., Lena, A., Helio, A.F. 2015. Understanding knowledge leakage: a review of previous studies, *VINE*, 45(4): 568-586.
- Tang, J., Cui, Y., Li, Q., Ren, K., Liu, J. & Buyya, R. 2016. Ensuring security and privacy preservation for cloud data services. *ACM Computing Surveys (CSUR)*, 49(1): 13-39.
- Tang, M. & Zhang, T. 2016. The impacts of organizational culture on information security culture: a case study. *Information Technology and Management*, 17(2):179-186.
- Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J. & Cotten, S. R. 2016. Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, 59, 138-150.
- Twum-Darko, M., 2014. Factors influencing readiness for transformational EGovernment.pdf. *Journal of Public Administration*,1–12.
- Tohidinia, Z. & Mosakhani, M., 2010. Knowledge sharing behaviour and its predictors. *Industrial Management & Data Systems*, 110(4): 611–631.
- Twum-Darko, M. & Harker, L.-A.L., 2014. Factors influencing knowledge sharing 148 amongst higher education academics at a university in South Africa.1–14.
- Tsohou, A., Karyda, M. & Kokolakis, S. 2015. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. *Computers & security*, 52,128-141.
- Underhill Corporate Solutions. 2011. Literature review on small and medium enterprises' access to credit and support in South Africa. Pretoria. Report prepared for the National Credit Regulator.
- Vance, A., Lowry, P.B. & Eggett, D. 2013. Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, 29 (4): 263-290.
- Vezzetti, E., Violante, M.G. & Marcolin, F. 2014. A benchmarking framework for product lifecycle management (PLM) maturity models. *The International Journal of Advanced Manufacturing Technology*, 71 (5-8): 899-918.
- Villa, Y. & Johnson, A.S. 2014. Assessing risk of information leakage, patents, Grant. U.S. Vrije Universiteit Amsterdam, 2015. Available at <https://vu.nl/en/programmes/links/application.aspx>, accessed, 18 December 2016.
- Wahyuni, D. 2012. The research design maze: Understanding paradigms, cases, methods and methodologies, 10(1): 69-80.
- Walsham, G. 1995. The emergence of Interpretivism in IS research. *Information Systems Research*, 6(4):376-394.
- Whitman, E. & Mattord, H. J. 2012. Management of Information Security. Boston, Massachusetts: *Thomson Course Technology*, 36(3): 363-375.

- Whitman, M.E., Coles, M.J. & Mattord, H.J. 2012. Principles of information Security. 4th edition. London: Cengage Learning.
- Xavier, S.M., Kelley, D., Kew, J., Herrington, M. & Vorderwülbecke, A. 2012. Global Entrepreneurship Monitor: 2012 Global Report. Available at <http://www.gemconsortium.org/docs/download/2645>. [19 December 2016]
- Xu, S., Meso, P. & Ding, Y. 2016. Information Security Training Customized by Risk Profile. In the proceedings of Twenty-second Americas Conference on Information Systems, San Diego: USA.
- Yildirim, E. 2016a. Advances in Human Factors in Cybersecurity. Florida, USA
- Yildirim, E. 2016b. The Importance of Information Security Awareness for the Success of Business Enterprises. *Advances in Human Factors in Cybersecurity*, 501, 211-222.
- Yin, R. 2013. Case Study Research: Design and Methods. California : Sage.
- Yin, R. K. 2009. Case study research: Design and methods (4th ed.). Thousand Oaks, Calif.: Sage.
- Yang, H.L. & Wu, T.C.T., 2008. Knowledge sharing in an organization. *Technological Forecasting and Social Change*, 75(8): 1128–1156.
- Yu, D. & Yang, J. 2017. An Integrated Management Model for Avoiding Customer Information Leakage in China's Housing Markets, *Journal of the Knowledge Economy*, 1-25.
- Yunis, M., El-Kassar, A.N., Tarhini, A. 2017. "Impact of ICT-based innovations on organizational performance: The role of corporate entrepreneurship", *Journal of Enterprise Information Management*, 30(1):122-141
- Yunos, Z., Ab Hamid, R.S. & Ahmad, M. 2016. Development of a cyber-security awareness strategy using focus group discussion. In SAI Computing Conference (SAI), 1063-1067 IEEE.
- Zhang, Y. & Wildemuth, B. M. 2009. Qualitative analysis of content. In B. Wildemuth (ed.), *Applications of social research methods to questions in information and library science*: 308-319. Westport, CT: Libraries Unlimited.
- Zikmund, W.G., Babin, B.J., Carr, J.C. & Griffin, M. 2010. Business research methods. 8th ed. South-Western: Cengage Learning.

Appendix A: Introductory Letter for Data Collection



Introductory letter for the collection of research data

Mr Steven Lububu is registered for the M Tech (IT) degree at CPUT student number 209002409. The thesis is titled "*the perception of employees concerning ISP compliance: case studies of a European (VU Amsterdam) and South African University (CPUT),*" and aims to understand users' perceptions about ISP and resulting information security behaviours towards ISP compliance within the selected universities. And to establish a framework which complies with ISP compliance at Individual level within the institution with low (CPUT) and high privacy controls (VU Amsterdam) by interconnecting both universities to exchange cultures between them.

The supervisor(s) for this research is: Dr Pieter Wagenaar. Contact details: VU Amsterdam, Tel: 0031 205986918. Email: f.p.wagenaar@vu.nl

In order to meet the requirements of the university's Higher Degrees Committee (HDC) the student must get consent to collect data from organisations which they have identified as potential sources of data. In this case the student will use interview technique(s) to gather data.

If you agree to this, you are requested to complete the attached form (an electronic version will be made available to you if you so desire) and print it on your organisation's letterhead. For further clarification on this matter please contact either the supervisor(s) identified above, or the Faculty Research Ethics Committee secretary (Ms V Naidoo) at 021 469 1012 or naidoove@cput.ac.za.

Yours sincerely

Dr Pieter Wagenaar

13 October 2015

Appendix B: Permission to Conduct Institutional Research –Vu Amsterdam

Permission to conduct Institutional research – VU Amsterdam: Mr Steven Lububu

I, Peter Kerkhof, in my capacity as chair of the department of Communication Science at VU Amsterdam University, give consent in principle to allow Mr Steven Lububu, a student at the Cape Peninsula University of Technology, to collect data in this company as part of his M Tech (IT) research. The student has explained to me the nature of his research and the nature of the data to be collected.

This consents in no way commits any individual staff member to participate in the research, and it is expected that the student will get explicit consent from any participants.

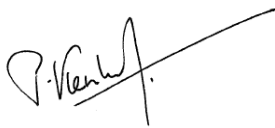
I reserve the right to withdraw this permission at some future time.

In addition, the company's name may or may not be used as indicated below. (Tick as appropriate.)

	Thesis	Conference paper	Journal article	Research poster
Yes	√	√	√	√
No				

Peter Kerkhof

20-10-2015



Appendix C: Official Invitation for Mr. Steven L. Lububu

Date our reference enclosure(s)

12 august 2015

Your letter dated your reference

Telephone fax email

(020) 59 87737 (020) 598 6765 c.c.j.gerards@vu.nl

Mailing address: savusa, cis centre for international cooperation, de boelelaan 1105,
1081hv amsterdam

The Dutch Embassy in South Africa

PO Box 117 Pretoria 0001

South Africa



Subject: **Official invitation for Mr. Steven I. Lububu**

To whom it may concern,

The Faculty of Social Sciences of VU University Amsterdam, would like to officially invite Mr. Steven Lububu (passport number: 0B0436505) for an intensive period of research and data collection for his Master thesis entitled: "Perceptions of employees concerning information security policy compliance: case studies of a European and South African university" in the period from 01 November 2015 – 29 January 2016. Mr. Lububu is a Master's student from The Cape Peninsula University of Technology's Department of Informatics and Design.

Mr. Lububu intends to visit VU University for data collection and supervision by Dr. Pieter Wagenaar. The Cape Peninsula University of Technology has offered Mr. Lububu a scholarship to cover his visa, travel, food, insurance and accommodation costs.

If you have any further questions please do not hesitate to contact us.

Thanking you very much in advance.

With kind regards,

Dr. F. Pieter Wagenaar

A handwritten signature in black ink, appearing to read 'F. Pieter Wagenaar', written over a horizontal line.

Department of Political Science and Public Administration VU University
Amsterdam

Appendix D: Interview Schedule for Top Management

Semi-structured questions

Interview Question (IQ)

Research Main Question	How can the non-compliance with information security policies by employees in an institution be managed?
Research sub-question 1	How is InfoSecPol enforced in institutions?
IQ1	In your opinion, how to enforce the policies of this institution?
Answer	
IQ2	Based on your experience, to what extent are the policies of this university enforced?
Answer	
IQ3	How do you enforce the policies with regards to your employees?
Answer	
IQ4	Why are InfoSecPols enforced?
Answers	
IQ5	Are you aware of the policy of this university? If yes please explain, if no, why not?
Answers?	
IQ6	Do you communicate often with your employees about the policy? If yes how? If not, why not?
Answers	
IQ7	Tell me about InfoSecPol according to your own understanding?
Answers	
Research sub-questions 2	What are the factors that influence non-compliance with InfoSecPol?
IQ1	In your opinion, would you tell me the factors that influence information leakage?
Answers	
IQ2	Based on your experience, to whom the factors that influence information leakage are significant?
Answers	
IQ3	How are the factors of information leakage significant to a third party?

Answers	
IQ 4	Why are the factors of information leakage significant to a third party?
Answers	
IQ 5	In your opinion, how can one avoid intentional or unintentional leakage in this institution?
Answers	
IQ6	In your opinion, what could be the causes of information leakage?
Answers	
IQ7	How are the factors of information leakage interpreted to your employees?
Answers	
IQ8	Do you communicate often with your employees about the consequences related to non-compliance with policies? If yes how? If not, why not?
Answers?	
IQ9	In your opinion, what could be the consequences related to non-compliance with policies?
Answers	
IQ10	Based on your experience, what could be the causes of breaking the rules in this institution?
Answers?	
IQ11	In your opinion, what prevents you or your employees from complying with InfoSecPols?
Answers	
Sub-Question3	What are the factors that influence compliance with InfoSecPol?
IQ1	In your opinion, what factors influence your compliance with InfoSecPol?
Answer	
IQ2	Based on your experience, who are the factors that influence InfoSecPol compliance significant to?
Answers	
IQ2	How do you comply as a manager of this department?
Answers	
IQ3	Do you comply with your policies? If yes, how? If not, why not?
Answer	

IQ3	Based on your experience, how do you understand the factors that lead to compliance?
Answers	
IQ4	In your point of view, how are the factors of compliance significant to you and your institution?
Answer	
IQ5	Why are the factors of compliance significant to you and your institution?
Answers	
IQ4	Are the policies of this university beneficial to you? If yes how. If not, why not?
Answer	
IQ5	How do you support and promote factors that influence compliance in this institution?
Answers	
IQ6	How do you interpret the factors that influence compliance to your employees?
Answer	
IQ7	Why are factors of compliance interpreted to your employees?
Answers	
IQ8	What could influence your feelings to comply with InfoSecPol?
Answers	
IQ9	What motivates you to comply?
Answers	
IQ10	How do you communicate the factors that influence compliance with your employees?
Answer	
IQ11	Why are the factors of compliance communicated with your employees?
Answers	

Appendix E: Interview Schedule for Staff Members

Semi-structured questions

Interview Question (IQ)

Research Main Question	How can the non-compliance with information security policies by employees in an institution be managed?
Research sub-question 1	How are InfoSecPols enforced in institutions?
IQ1	In your opinion, how are the policies enforced in this university?
Answer	
IQ2	Based on your experience, to what extent are the policies of this university enforced?
Answer	
IQ3	How are the policies enforced with regards to your compliance?
Answer	
IQ4	In your opinion, why are InfoSecPol enforced?
Answers	
IQ5	Are you aware of the policy of this university? If yes please explain, if no, why not?
Answers?	
IQ6	Do you communicate often with your managers about the policies? If yes how? If not, why not?
Answers	
IQ7	Explain InfoSecPol, according to your own understanding.
Answers	
Research sub-questions 2	What are the factors that influence non-compliance with InfoSecPol in an institution?
IQ1	In your opinion, what are the factors that influence information leakage?
Answers	

IQ2	Based on your experience, to whom the factors that influence information leakage are significant?
Answers	
IQ3	How are the factors of information leakage significant to a third party or cybercriminals?
Answers	
IQ 4	Why are the factors of information leakage significant to a third party?
Answers	
IQ 5	In your opinion, how can one avoid intentional or unintentional leakage in this institution?
Answers	
IQ6	In your opinion, what could be the causes of information leakage?
Answers	
IQ7	How do you understand the factors that influence information leakage?
Answers	
IQ8	Are you aware of the consequences related to non-compliance with policies? If yes how? If not, why not?
Answers?	
IQ9	In your opinion, what could be the consequences related to non-compliance with policies?
Answers	
IQ10	Based on your experience, what could be the causes of breaking the rules in this institution?
Answers?	
IQ11	In your opinion, what prevents you or your institution from complying with InfoSecPol?
Answers	
Sub-Question3	What are the factors that influence compliance with InfoSecPol?
IQ1	In your opinion, what are the factors that influence your compliance?
Answer	
IQ2	Based on your experience, to whom the factors that influence information security policies compliance are significant?
Answers	

IQ2	How do you comply as a staff member?
Answers	
IQ3	Do you comply with your policies? If yes how? If not, why not?
Answer	
IQ3	Based on your experience, how do you understand the factors that lead to compliance?
Answers	
IQ4	In your point of view, how are the factors of compliance significant to you and your institution?
Answer	
IQ5	Why are the factors of compliance significant to you and your institution?
Answers	
IQ4	Are the policies of this university beneficial to you? If yes how. If not, why not?
Answer	
IQ5	How do you support and promote factors that influence compliance in this institution?
Answers	
IQ6	How do you interpret the factors that influence compliance?
Answer	
IQ7	How are the factors of compliance interpreted to you by the managers?
Answers	
IQ8	What could influence your feelings to comply with InfoSecPol?
Answers	
IQ9	What motivates you to comply?
Answers	
IQ10	How do you communicate the factors that influence compliance with your colleagues or managers?
Answer	
IQ11	Based on your experience, why are the factors of compliance communicated with your colleagues or managers?
Answers	

Appendix F: Transcription for Top Management

Participant 1

Rank: Manager

Institution: V1

Research Question	Main	How can the non-compliance with information security policies by employees in an institution be managed?
Research question 1	sub-	How is information security policies enforced in institutions?
IQ1		In your opinion, how to enforce the policies of this institution?
Answer		Creating (InfoSecPol) is the first step in securing and enforcing. Second step is to increase of awareness of security risks. Also, training and education on how to protect information enforce the existing policies. The third step is to implement technology that controls and monitor the system.
IQ2		Based on your experience, to what extent are the policies of this university enforced?
Answer		Encryptions and description techniques should be applied to enforce the security of information. The sanction must be given to the transgressors.
IQ3		How do you enforce the policies with regards to your employees?
Answer		We initiate workshops, and training for our staff members. And ourselves of course. Smiles...
IQ4		Why information security policies are enforced?
Answers		Information security policies are enforced to improve the security of information. The security of information must be enforced in all aspects including technologies and human actors' interactions.
IQ5		Are you aware of the policy of this university? If yes please explain, if no, why not?
Answers?		YES, I am aware of the policies. Information security is a set of rules, instructions and guidelines given to protect information and information resources. In this institution we policies on hardware and software, policies email or phishing and policies related to protecting students' information. Students' information cannot be disclosed unofficially.
IQ6		Do you communicate often with your employees about the policy? If yes how? If none, why not?

Answers	Not really, each department has to communicate with the staff members about the policies. To be honest with you I never done it but we do have the policies. We do communicate with a staff about the policies only the first day of his/her employment. Smile....
IQ7	Tell me about InfoSecPol according to your own understanding?
Answers	ISP is about the protection of information from unauthorised people.
Research sub-questions 2	What are the factors that influence non-compliance with InfoSecPol in institutions?
IQ1	In your opinion, would you tell me the factors that influence information leakage?
Answers	Hum....such thing never happened here in Netherlands but I can have ideas. Lack of awareness, insufficiency of resources, lack of communication of course (smile). For example here we do not have enough store rooms to keep students' theses or exam papers. The policy does not allow us to keep students' work in our office but I am doing it. I have lot of documents here (smile). Fraud, corruption, lack of transparency and so on.
IQ2	Based on your experience, to whom the factors that influence information leakage are significant?
Answers	These factors are beneficial to criminals or third party. In my case I am not a criminal but I do not comply because the university does not provide enough store rooms for us. I do not have any choice right now. I have to keep these documents in my office for the security purposes of information.
IQ3	How the factors of information leakage are significant to third party?
Answers	For their incentive, competition on the market, sabotage and leadership.
IQ 4	Why the factors of information leakage are significant to third party?
Answers	I said it ready..... For their incentive, competition on the market, sabotage and leadership
IQ 5	In your opinion, How to avoid intentional or unintentional leakage in this university?

Answers	Not leaving your PC unattended, not leaving your office unattended, frequently changing passwords, awareness of security threats is also an advantage, not talking to much about yourself or your organisation (smile)....
IQ6	In your opinion, what could be the causes of information leakage?
Answers	Incentive issues, lack of awareness of IS threats, insufficiency of resources, lack of communication and inexperienced IT staff members.
IQ7	How the factors of information leakage are interpreted to your employees?
Answers	These factors can be interpreted in terms of security education, awareness and training. By giving instruction and knowledge to employees on how to avoid information leakage intentionally or unintentionally.
IQ8	Do you communicate often with your employees about the consequences related to non-compliance with policies? If yes how? If none, why not?
Answers?	Not often but we do during security meetings and workshops. But our university has a committee which is in charge of providing awareness programme to our staff members.
IQ9	In your opinion, what could be the consequences related to non-compliance with policies?
Answers	Inability to sustain, to reach the objectives and goals, inability to function and compete on the market. Also organisation can close down. Or been fired by the organisation.
IQ10	Based on your experience, what could be the causes of breaking the rules in this institution?
Answers?	When university does not comply with the policies on availability of infrastructure (smile), lack of social environment.
IQ11	In your opinion, What prevent you or your employees from complying with InfoSecPol's?
Answers	Lack of social environment or insufficiency of resources
Sub-Question3	What are the factors which influence information security policies compliance?
IQ1	In your opinion, would you tell me the factors that influence your compliance?

Answer	Awareness of policies, communication, preventive security systems to monitor and control the network,
IQ2	Based on your experience, To whom the factors that influence information security policies compliance are significant?
Answers	These factors are significant to employees and other relevant users of information
IQ2	How do you comply as a manager of this department?
Answers	How do I comply?....hum.....My sense of responsibility, commitment, value of information and belief.
IQ3	Do you comply with your policies? IF yes How? IF none, why not?
Answer	YES I do..... but not 100% (smile). The information has a value and I do believe that such value has to be protected. The value of information is connected to its security.
IQ3	Based on your experience, how do you understand the factors that lead to compliance?
Answers	The factors of compliance lead to the protection of information.
IQ4	In your point of view, How factors of compliance are significant to you and your university?
Answer	The factors of compliance increase employees' knowledge on how to protect information and prevent leakage.
IQ5	Why factors of compliance are significant to you and your University?
Answers	These factors motivate me, instruct and give me ideas on how to protect information. These factors are significant to the university for its sustainability, functionality and productivity.
IQ4	Are the policies of this university beneficial to you? If yes How, IF none, why not?
Answer	YES....they are beneficial. They guide and instruct us on how to behave and conduct ourselves at workplace.
IQ5	How do you support and promote factors that influence compliance in this university?
Answers	We do support by initiating security meetings and workshops.
IQ6	How do you interpret the factors that influence compliance to your employees?

Answer	They are interpreted as security education and procedures to compliance with policies
IQ7	Why factors of compliance are interpreted to your employees?
Answers	They are interpreted for improving security of information, protecting information resources, promoting security culture in this university and improving behaviour change towards compliance with policies.
IQ8	What could influence your feeling to comply with InfoSecPol?
Answers	Awareness, responsibility and commitment
IQ9	What motivate you to comply?
Answers	I said it ready (smile)
IQ10	How do you communicate the factors that influence compliance with your employees?
Answer	The factors of compliance are communicated as security education. These factors provide skills and knowledge needed to employees on how to protect and avoid leakage.
IQ11	Why the factors of compliance are communicated with your employees?
Answers	To secure information and information resources

Appendix G: Transcription for Staff Members

Participant

Rank: Secretary

Institution: C15

Research Main Question	How can the non-compliance with information security policies by employees in an institution be managed?
Research sub-question 1	How is information security policies enforced in institutions?
IQ1	In your opinion, how are the policies enforced in this university?
Answer	I don't have any ideas (smile)
IQ2.	Based on your experience, to what extent are the policies of this university enforced?
Answer	Encryption of information, and changing the password frequently> this is what I know from this university.
IQ3	How are the policies enforced with regards to your compliance?
Answer	I cannot disclose students' information unofficially.
IQ4	In your opinion, Why information security policies are enforced?
Answers	I think that the institution wants to protect information. The information has a value.
IQ5	Are you aware of the policy of this university? If yes please explain, if no, why not?
Answers?	Not at all. The policies exist but they never been communicated to us.
IQ6	Do you communicate often with your managers about the policies? If yes how? If none, why not?
Answers	I do communicate with the managers because I am a secretary. But we do not communicate based on the policies. There is a lack of communication between the management and staff members in terms of policies.
IQ7	Tell me about InfoSecPol according to your own understanding?
Answers	Protection of sensitive information
Research sub-questions 2	What are the factors which influence information leakage in organizations?

IQ1	In your opinion, would you tell me the factors that influence information leakage?
Answers	Lack of communication of the policies, lack of awareness of the policies, fraud, corruption and favouritism in this place.
IQ2	Based on your experience, to whom the factors that influence information leakage are significant?
Answers	These factors are significant to bad people who are stealing information unofficially. This is happening here often. Students are getting unofficial results and start complaining.
IQ3	How the factors of information leakage are significant to third party or cybercriminals?
Answers	For their happiness, incentive or business
IQ 4	Why the factors of information leakage are significant to third party?
Answers	For instance, in this institution students get unofficial results from authorised people who are working for the university. The system is not that secured. We cannot trust IT people in this institution. They are always leaking information.
IQ 5	In your opinion, How to avoid intentional or unintentional leakage in this university?
Answers	Changing frequently passwords, awareness of the policies, sanction leakers and make the rules on information leakage to be strict.
IQ6	In your opinion, what could be the causes of information leakage?
Answers	Students do not have money to pay in order to get the results. So, they have to hack the system. Insufficiency of resources, lack of experienced IT staff members and lack of transparency.
IQ7	How do you understand the factors that influence information leakage?
Answers	I do understand the factors that influence leakage as security breach and violation of the rules.
IQ8	Are you aware of the consequences related to non-compliance with policies? If yes how? If none, why not?
Answers?	YES.... I am. There is loss of information

IQ9	In your opinion, what could be the consequences related to non-compliance with policies?
Answers	The consequences are various such as losing the information and this can affect your work.
IQ10	Based on your experience, what could be the causes of breaking the rules in this institution?
Answers?	Students do not have money to pay in order to get the results. So, they have to hack the system. Insufficiency of resources, lack of experienced IT staff members and lack of transparency. Also there is a lack of leadership skill in this institution. Favouritism is a major problem.
IQ11	In your opinion, What prevent you or your institution from complying with InfoSecPol?
Answers	I do comply but the university does not. We do not have sufficient facilities to perform our work. We are very limited in terms of resources and facilities.
Sub-Question3	What are the factors which influence information security policies compliance?
IQ1	In your opinion, would you tell me the factors that influence your compliance?
Answer	Responsibility, commitment, transparency, attitude towards compliance , communication and awareness I can say so (smile....)
IQ2	Based on your experience, to whom the factors that influence information security policies compliance are significant?
Answers	To employees and other staff members
IQ2	How do you comply as a staff member?
Answers	Sense of responsibility and feeling of been employed and attitude towards compliace
IQ3	Do you comply with your policies? IF yes How? IF none, why not?
Answer	YES I do but partially..... (smile)
IQ3	Based on your experience, how do you understand the factors that lead to compliance?
Answers	I do understand them as security of information that leads to compliance.

IQ4	In your point of view, How factors of compliance are significant to you and your university?
Answer	Safety of private and institutional properties
IQ5	Why factors of compliance are significant to you and your University?
Answers	These factors instruct and lead to compliance as I said previously
IQ4	Are the policies of this university beneficial to you? If yes How, IF none, why not?
Answer	No they are not beneficial because they are not communicated to me.
IQ5	How do you support and promote factors that influence compliance in this university?
Answers	I do not support or promote but I do what is good for the university and me. This is the job for the management to support and promote. My contribution is to provide a good service (smile)
IQ6	How do you interpret the factors that influence compliance?
Answer	I do interpret them as security of information
IQ7	Why factors of compliance are interpreted to you by the managers?
Answers	Sorry dude, managers never interpreted any factors of compliance to us.
IQ8	What could influence your feeling to comply with InfoSecPol?
Answers	My personality and professionalism
IQ9	What motivate you to comply?
Answers	I am qualified for this position. (smile)
IQ10	How do you communicate the factors that influence compliance with your colleagues or managers?
Answer	N/A
IQ11	Based on your experience, Why the factors of compliance are communicated with your colleagues or managers?
Answers	To be honest with you we do not discuss about security issues between us staff members. We leave this to IT people (smile.....). But as an It assistant I know that the factors of compliance provide skills and knowledge about security threats.