Addressing ambiguity within Information Security Policies in Higher Education to Improve Compliance

by

Mokateko Portia Buthelezi

submitted in accordance with the requirements for
the degree of

MASTER OF SCIENCE

In the subject

COMPUTING

at the

University of South Africa

Supervisor: Prof. J.A. van der Poll

Co-supervisor: Mr E.O. Ochola

June 2017

Declaration

Student number: 47361921

I declare that the work contained in *Reviewing ambiguity within Information Security Policies to Improve Compliance* is my own work and that all the sources that were quoted or used have been indicated and acknowledged in the form of complete references.

______________________________ __09 June 2017__________________

Ms Mokateko Portia Buthelezi Date

Abstract

Information security (InfoSec) policies are widely used by institutions as a form of InfoSec control measure to protect their information assets. InfoSec policies are commonly documented in natural language, which is prone to ambiguity and misinterpretation, thereby making it hard, if not impossible, for users to comply with. These misinterpretations may lead the students or staff members to wrongfully execute the required actions, thereby making institutions vulnerable to InfoSec attacks. According to the literature review conducted in this work, InfoSec policy documents are often not followed or complied with; and the key issues facing InfoSec policy compliance include the lack of management support for InfoSec, organisational cultures of non-compliance, intentional and unintentional policy violation by employees (the insider threat), lack of policy awareness and training as well as the policy being unclear or ambiguous. This study is set in the higher education context and explores the extent to which the non-compliance problem is embedded within the policy documents themselves being affected by ambiguity.

A qualitative method with a case study research strategy was followed in the research, in the form of an inductive approach with a cross-sectional time horizon, whereby a selection case of relevant institutional InfoSec policies were analysed. The data was collected in the form of academic literature and InfoSec policies of higher education institutions to derive themes for data analysis. A qualitative content analysis was performed on the policies, which identified ambiguity problems in the data. The findings indicated the presence of ambiguity within the policy documents, making it possible to misinterpret some of the policy statements. Formal methods were explored as a possible solution to the policy ambiguity. A framework was then proposed to address ambiguity and improve on the clarity of the semantics of policy statements. The framework can be used by policy writers in paying attention to the presence of ambiguity in their policies and address these when drafting or revising their policy documents.

Keywords- Formal methods, Policy ambiguity; Usable security; Policy clarity; Policy human aspects; Security policy compliance

Acknowledgements

I am grateful for every contribution that made it possible for me to conduct this research study. I would like to say thank you to the following people: First and foremost, my supervisors, for their continued patience and support throughout the course of the study. Thank you. Thank you to Laetitia Bedeker for the professional language editing services.

A very special thank you to the University of South Africa Research Directorate for the resources made available to conduct this research, including the research funding.

Thank you to my husband, Bab'uShenge, for holding my hand during the course of the study and having to repeatedly listen to the same discussions. To my children, Nicola, Muziwandile, Otshepegile, Nathan, Areka, Lesego, Lesedi, Lentswe, Tumelo, Khwezi and Mpendulo, for taking it easy on me when I had to study, although some of you demanded compensation for lost time.

Thank you to my biological, adopted and academic families for your love and prayers. To my sisters, thank you for the encouragement, guidance sessions and sustaining a positive environment during my studies; the meals we had were not in vain.

To my mother, Sister Joey, your own progress kept me going, your support kept me sane, you are my hero. You will be the only person obliged to read this document in full for recreational purposes.

Most of all, I thank God for the patience to wait on Him, the wisdom to keep going and the strength to complete the work.

Dedication

I dedicate this research to the loving memory of my confidant, Cate Hlongoane Maribe: Thank you for always believing that I could do anything and do it well. Your faith in me was humbling. You actively supported me until your last day.

Peer reviewed publication from this research

The following publications emanated from this research, and were published in peer reviewed conference proceedings:

Buthelezi, M.P., User Online Information Security Practices: The South African Context. *In Proceedings of the International Conference on Cryptography and Security (ICCS)*, 2014, 18-23, ISBN: 978-81-925233-5-4.

Buthelezi, M.P., Van Der Poll, J.A. and Ochola, E.O., 2016, December. Ambiguity as a Barrier to Information Security Policy Compliance: A Content Analysis. *In Computational Science and Computational Intelligence (CSCI), 2016 International Conference*. Las Vegas, 2016, December, pp. 1360-1367, IEEE. ISBN: 978-1-5090-5510-4.

Table of contents

List of abbreviations

e-learning: Electronic learning.

ICT: Information and communications technology.

InfoSec: Information security.

ODL: Open distance learning.

PRQ: primary research question.

RO: Research objectives.

List of figures

List of tables

Chapter 1
Introduction to the study

1.1. Introduction

This is a dissertation on information security (InfoSec) policies and the challenges associated with the policy usage. Most higher learning institutions have adopted the use of mobile and electronic devices for teaching and learning (Defta, 2011). The use of electronic devices for educational purposes is referred to as electronic learning (e-learning) (Dabbagh & Kitsantas, 2012). While adopting the e-learning pedagogy, the institutions of higher learning also have had to take into consideration the need for InfoSec measures to protect the institutional data on the electronic platforms (Buthelezi & Mujinga, 2013). The institutional data could be in the form of student assignments submitted, student grades or it could be student and staff personal details.

The protection of institutional data for e-learning purposes has persuaded the researcher to investigate the InfoSec policies of higher education institutions, their contents and the challenges that face the policy usage. The next section provides the general background on information security.

1.2. Information security background

Security is the concept of feeling secure or safe from harm and danger (Whitman & Mattord, 2012). InfoSec is a concept centred on protecting the organisation's information and human resources by way of monitoring and compliance assessments (Gelbstein, 2006). Furthermore, InfoSec focuses on preserving the critical characteristics of information, such as availability, accuracy, authenticity, confidentiality and integrity (Whitman & Mattord, 2012). Given the growing importance of information, it is often viewed as being analogous to an organisation's key resource (Doherty, Anastasakis & Fulford, 2009). In the information and technology era where online presence and social media presence are important, information is indeed a key resource in any organisation. According to Peppard (2007), many executive teams have acknowledged the importance of information and that it ought to be managed efficiently.

Based on the importance placed on organisational information, it has become essential to put measures in place to safeguard such information. It becomes evident why there is a great need for information to be secured and effectively so, as access to organisational information has to be tightly controlled. Knapp, Morris, Marshall & Byrd, (2009) agree that organisations are more dependent on the reliability of their information systems in order to ensure the credibility of their information and decisions. This information includes trade secrets, patented ideas, patterns and recipes. What, for instance, would happen to the Coca cola beverage company, if consumers knew how to recreate their soft drinks in their own homes? This is the type of damage that could befall an organisation if its information is not effectively protected. Therefore, there is a need for InfoSec measures.

The InfoSec measures include defining the rules to govern the way in which organisational information should be secured or protected; such governing rules are the contents of InfoSec policies (Doherty, Anastasakis & Fulford, 2009). InfoSec policies are used as controls in the risk-management field of information technology (IT). Höne & Eloff (2002) further reiterated that InfoSec policies act as controls to manage InfoSec in an organisation. The state of InfoSec in an organisation is often measured against the InfoSec policy as an organisational benchmark. The organisation has to ensure that the InfoSec policy is available to its intended users, reasonably easy to use, regularly updated and kept current (Gelbstein, 2006). InfoSec policies allow for the tracing and preserving of the information characteristics that could be compromised if or when the information is accessed and tampered with.

There is currently widespread use of information and communications technology (ICT) such as mobile phones, laptops and tablet devices. These ICT devices can be used for a variety of activities, from accessing study material to online shopping and social networking with the aid of an internet connection. When using the ICT devices on the internet (online), users often share and exchange personal information with others (Gelbstein, 2006).

The online information exchange could be intercepted and used for unauthorised purposes by malicious users (Knapp, Morris, Marshall & Byrd, 2009). Therefore, there is a need for policies to guide the technology users on how to protect their personal information as well as institutional information from unauthorised access. Corporate organisations have these guidelines written in their information security (InfoSec) policy document, and so do Higher learning institutions (Peppard, 2007).

Although it remains the responsibility of the users to protect their personal information when using technology, the organisations provide the policy as a security control to guide the users on the organisational ICT infrastructure and what the organisation deems acceptable use of the information assets (Whitman & Mattord, 2012).

The InfoSec policy document should be made available to all employees who will be granted access to organisational information resources (system users). The system users are to read and acknowledge that they have read, accepted and understood the contents of the InfoSec policy (Whitman & Mattord, 2012).

The InfoSec policy document also states the user roles and responsibilities in protecting the organisational information. On the other hand, the user privileges would be the type of access that the user has been granted, on each system available to them. The privileges are documented in the system security policies in the form of configurations and settings (Knapp, Morris, Marshall & Byrd, 2009). The next section discusses the InfoSec policy document in detail.

1.2.1. The information security policy document

The InfoSec policy document is a security control that is used to preserve the confidentiality, integrity and authenticity of information (Whitman & Mattord, 2012). The confidentiality can be preserved by ensuring only authorised users have access to the information (Gelbstein, 2006). The integrity can be preserved by ensuring that only the authorised users can make changes to the information; and the authenticity can be maintained by making sure that the system users are indeed who they claim to be.

To ensure authenticity, users are typically authenticated with the use of a username and password credentials before they can access the information system (Peppard, 2007; Andress, 2014). Once a user has been authenticated with a username and password (user profile), any subsequent actions performed by that user profile on any information system, would be referred to as the actions performed by that particular user (Whitman & Mattord, 2012). This means that all the system users will be held responsible for any actions performed using their user profile.

In the case where system users have shared or disclosed their password to someone else, it means that the other person could gain access to the system pretending to be the authorised user. For this reason, the InfoSec policy would generally have a password management section where it provides the minimum requirements for a safe password also state that users should not share or disclose their passwords to anyone. The next section discusses InfoSec policy compliance.

1.2.2. Information security policy compliance

InfoSec policies define the rules that govern access to information and other resources belonging to an organisation. The defined rules detail the intended information resource users and their access rights and responsibilities. These policies are aimed at helping users understand what is deemed acceptable and responsible behaviour in handling organisational data and information to ensure the safe and secure handling of information in performing their organisational duties and responsibility (Höne & Eloff, 2002). There have been developments on what a good InfoSec policy should entail. One of the most recent ones is by Whitman & Mattord (2012). They describe the notion of a good InfoSec policy as one that encapsulates the responsibilities of individuals, indicates what is authorised and unauthorised system use and enables individuals to report suspected or identified threats (whistle blowing). Furthermore, it should define punishment means for policy violations and ways to update the policy to keep up with the constantly changing IT environment.

Employees should have no excuse for not being able to apply defined security practices in accordance with the established InfoSec policy (Saleh, Alrabiah & Saad, 2007). Hence there should be established InfoSec policies in place for employees to apply and adhere to. Subsequently, the InfoSec policy should act as the point of departure for employees to follow regarding all InfoSec issues, and in so doing; it becomes the ‘heart and basis’ of successful security management (Von Solms & Von Solms, 2004:374). With the InfoSec policy being referred to as the heart and basis of successful security management, it can be concluded that this document should be written in a manner that is comprehensible to all employees, similar to how the organisational values are documented, in simple, user-centred language.

1.2.3. Inconsistencies and information security policies

One of the main issues surrounding InfoSec policy compliance is that the InfoSec policies are generally documented in natural language, which is prone to ambiguity and inconsistencies (Andress, 2014). Kamsties & Paech (2000) postulate that although natural language is generally considered flexible, universal and wide-spread, documents that are in natural language are known to be inconsistent, incomplete and integrally ambiguous.

In order to understand the reported inconsistency problem within InfoSec policy documents, a sample of online InfoSec policy documents from institutions of higher learning were collected and reviewed. Among the collected documents was an, “*Information security best practice document*” (Information security best practice document, 2010).

While reviewing the *Information security best practice document* by (Information security best practice document, 2010:13), which should be a guiding document for InfoSec policies, the following inconsistencies were noted: The document stated in its classification and control of assets section that

> *“[a] plan for electronic storage of essential documentation should be developed”*. (Information security best practice document, 2010:13)

There was neither an indication of who (what role) should develop this plan, nor did it define or refer to a definition of what ‘essential documentation’ referred to. This made it open-ended and susceptible to misinterpretation. However, in the section on protection against malicious code, the same document stated that

> *“[c]omputer equipment must be safeguarded against virus and other malicious code. This is the responsibility of the IT security manager”.* (Information security best practice document, 2010:13)

In this section, the responsibility was clearly allocated and documented. There was a level of assumed, implicit knowledge in the first requirement and the latter requirement was explicitly stated in clear terms (Hostland, Enstad, Eilertsen & Boe, 2010). The above discussion leads to the following problem statement.

1.3. Problem statement

InfoSec policies could suffer from reduced clarity due to the policy documents not being coherent. Policy users tend to unintentionally breach the InfoSec policy because of misinterpreting the policy statements. The researcher departed from the premise that the InfoSec policies are prone to the lack of clarity. These policies are often documented in natural language, which renders some of the content ambiguous and subject to different interpretations. Andress (2014) reported an important aspect of InfoSec policies, namely that they should be kept current by means of periodic reviews and updates to ensure that they are relevant and applied by their intended users. Updates are often made when inconsistencies or conflicts are noted in the policy documents or to address new aspects that have been introduced by the constantly changing technology environment.

Doherty, Anastasakis & Fulford (2009) suggest that the most important role of the InfoSec policy is to make plain the rights and responsibilities of users such that these are made clear to and are understood by the users. This is to ensure that there is a uniform and consistent institutional view of InfoSec. This further points to the need to make InfoSec policies explicit, leading to the need to formalise them. Rees, Bandyopadhyay & Spafford (2003) arrived at a similar conclusion, pointing out the problem of keeping InfoSec policies consistent.

Generally, InfoSec policies are often documented in ambiguity-prone natural language (Parkin, Van Moorsel & Coles, 2009). The presence of ambiguity could lead to reduced clarity, which could lead the InfoSec policy users to incorrectly execute policy statements, thereby making it difficult to comply with the unclear policies.

There have been empirical contributions and academic discussions focussing on the content of InfoSec policies with reference to the topics addressed by the policy documents, but not on the clarity and consistency of the policy content detail, as observed from Olnes (1994), Pounder (2002) as well as Doherty, Anastasakis & Fulford (2009).

The next section provides the research aim and objectives compiled to address the research problem.

1.4. Research Aim and Objectives

1.4.1. Research Aim

The aim of the research is to conceptualise a framework for addressing university InfoSec policy ambiguity, to aid InfoSec policy compliance.

The research aim was broken down into achievable action items in the form of research objectives in the next section.

1.4.2. Research Objectives

In order to fulfil the research aim, the following research objectives (ROs) were derived:

RO1: Explore the literature on InfoSec policies;
RO2: Identify the main problems facing InfoSec policy compliance;
RO3: Identify the main problems relating to ambiguity within InfoSec policies;
RO4: Compile a framework on how InfoSec policy ambiguity can be reduced to improve compliance and clarity.

The next section provides the research questions used to address the research objectives.

1.5. Research questions

1.5.1. Main research question

To define and fulfil the objectives of this research, the following primary research question (PRQ) was formulated for the study:

PRQ: How can a framework for addressing university InfoSec policy ambiguity be conceptualised?

The next section provides the secondary research questions that were posed, in order to answer the PRQ in detail.

1.5.2. Secondary research questions

From the main research question, the following secondary research questions (SRQs) were derived:

SRQ1: What does literature on InfoSec policies say about InfoSec policy issues?

SRQ 2: What are the main problems with InfoSec policy compliance?

SRQ 3: What are the main problems relating to ambiguity within InfoSec policies?

SRQ 4: How can InfoSec policy ambiguities be reduced to improve policy compliance and clarity?

1.6. Study Location and Context

The study is located in the sub-Saharan country of South Africa, in the context of higher learning institutions.

One of the country’s biggest e-learning and open-distance learning (ODL) institutions was used for the research. The reason for the context was that as an ODL institution, most of its students studied online and needed to rely on the institution’s e-learning systems. The same reliance goes for the staff members for academic and administrative purposes.

The student and staff reliance of the e-learning systems therefore requires for them to familiarise themselves with the institutional InfoSec policies for guidance on using the e-learning system securely, and minimise security incidents. This research departs from the perspective of the staff members in the context of a higher education institution.

1.7. Significance of the study

InfoSec policies are the documents that help govern organisations' InfoSec. These are often ambiguous, as they are stated and documented in natural language, which is open to misinterpretation. Consequently, these policies could be bypassed by the intended users or misinterpreted, because the users could act based on the incorrect interpretation of the policy requirements. Users could therefore use other possible meanings of the policy requirement and not the interpretation that was intended by the policy owners, which may lead to a breach of policy. This could lead to the policy users exposing the institution to IT risks, thereby rendering it susceptible to InfoSec exploitation and possible attacks.

The researcher reviewed the contents of InfoSec policies for the existence of ambiguities and suggested a framework to reduce ambiguity in such policy statements. This research should make a contribution such that future InfoSec policies may be made clearer and therefore more comprehensible and easy to use. The practical contribution of this research would be a new framework for clarifying InfoSec policy documents, such that only one interpretation is understood from each policy statement with no alternative translations. This devised framework should facilitate policy and decision making in the InfoSec space and inform practice.

Oates (2009) echoes the view that research should be significant such that it brings about new theories or informs practice. The recommendations from this research could be used by InfoSec professionals in devising or enhancing their InfoSec policies. The theoretical contribution will be the compilation of a framework for reducing ambiguity within InfoSec policies, resulting in more comprehensible and precise policy requirements and thereby improved compliance with the InfoSec policies.

1.8. Research Methodology

This research used an interpretive philosophical paradigm and a qualitative research method with a case study research strategy was followed for this research in the form of an inductive approach with a short-term, contemporary time focus, also referred to as a cross-sectional time horizon as noted in Figure 1.1.

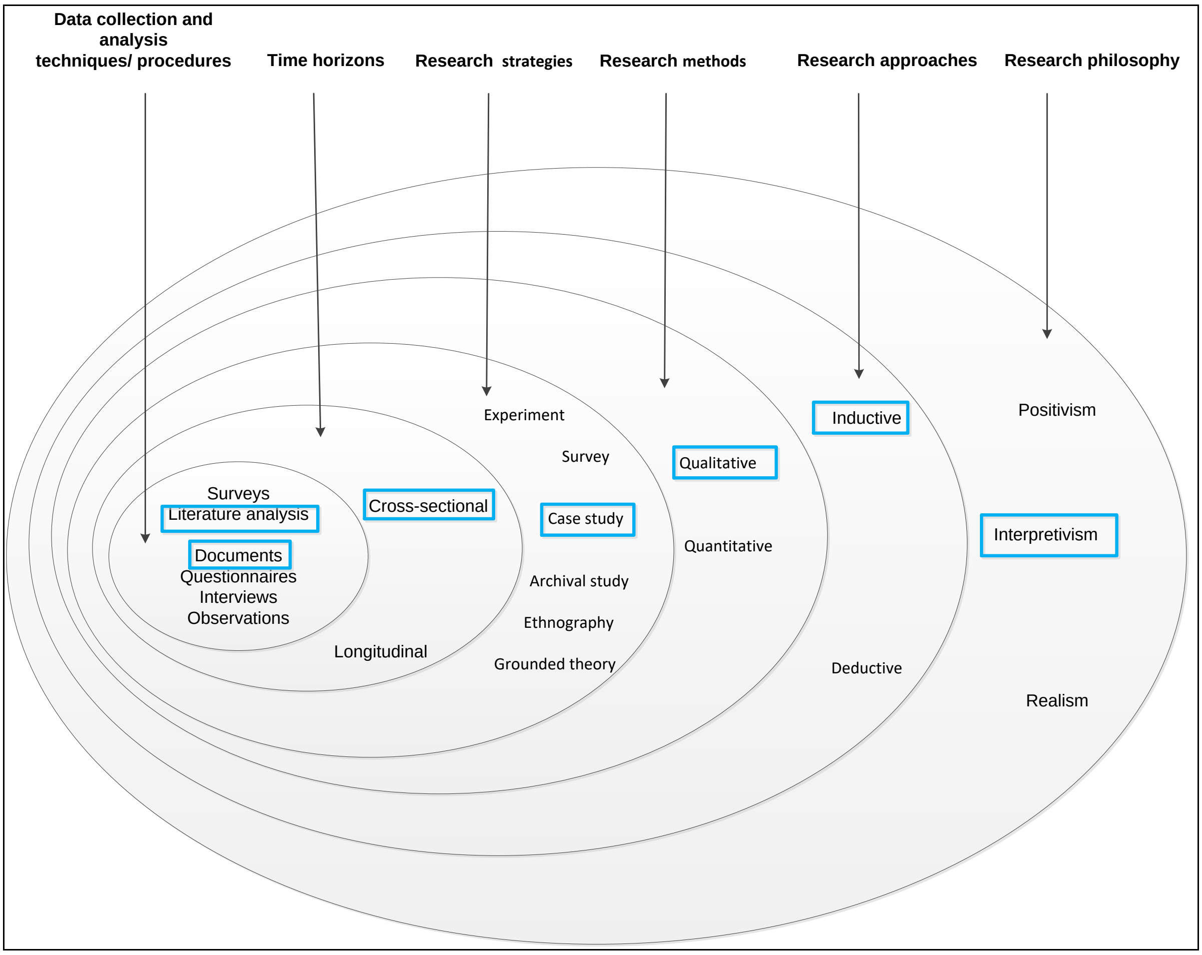


Figure 1.1: The research onion adapted from (Saunders, Lewis & Thornhill, 2009)

Figure 1.1 represents the research onion by Saunders, Lewis & Thornhill, (2009), which is commonly used to represent the research process. For this research project, the research process was as follows:

The aim of the research is to conceptualise a framework for addressing university InfoSec policy ambiguity, to aid InfoSec policy compliance. To achieve this, the researcher first had to investigate the existence of ambiguities within InfoSec policies and to explore how these occur and how the ambiguities pose a compliance problem.

The researcher conducted a systematic literature review and also collected institutional InfoSec policies online for an initial review, in order to identify the occurring themes. Part of the process in identifying the themes included analysing the policy statements for ambiguity, and determined whether different interpretations could be made from the policy requirement. Each identified type of ambiguity constituted a theme.

The identified themes were later used in reviewing the policy document samples from the sampled South African Higher Education institution. A framework of possible solutions to reduce ambiguity was drafted and documented in Chapter 5.

Using a literature review as well as content analysis is a form of triangulation that was used to ensure reliability of the findings.

The research data was collected in the form of a literature analysis of academic literature, as well as online existing InfoSec policy documents. A systematic literature search was first performed to gather background literature on the work performed in the area of InfoSec policy compliance and to identify a research gap that this research project could address (cf.

Stemler, 2001; Yin, 2009). This was followed by a qualitative content analysis to identify ambiguity problems as themes in the data (cf. Palinkas, Horwitz, Green, Wisdom, Duan & Hoagwood, 2015).

The content analysis centres its data collection on existing data sets or archival documents (Elo et al., 2015; Polit & Beck, 2012). When the data had been analysed and the ambiguity problem was evident, the researcher sought possible solutions to the identified ambiguity problems in the form of a set of steps to be followed per problem type. This process of seeking possible solutions resulted in a model built to address each identified ambiguity problem type.

The research methodology and research onion were discussed in detail in the research methodology chapter, chapter 3. The next section discusses the research limitations and delineations.

1.9. Limitations and delineations

The researcher anticipated that the institutional InfoSec IS policies would have some level of ambiguity and expected to improve the quality and comprehensibility of the said InfoSec IS Policies by devising a way to reduce the ambiguity. The researcher has noted that the current documentation of InfoSec policies is in the natural languages, which is susceptible to multiple interpretations.

This has led the researcher to further explore the details of these InfoSec policies and verify the existence of ambiguities. Subsequent to determining the existence of the ambiguities, a framework was developed for addressing the identified ambiguities. The ambiguities included identifying omissions and contradictions in the InfoSec policy documents. The presence of ambiguity could lead to reduced clarity, which could lead the InfoSec policy users to incorrectly execute policy statements, and thereby fore making it difficult to comply with the unclear policies. One of the limitations of the study is that the study was conducted by a single researcher due to the study being a dissertation.

The scope of this research is limited to user InfoSec policies and does not extend to the inclusion of system InfoSec policies. The next section presents the proposed contribution of the study.

1.10. Proposed contribution

The results of the study should inform practice in the field of InfoSec management, mainly the InfoSec manager in the process of developing, reviewing, updating and managing the InfoSec policy document. Managers can use this study as a reference point to begin the review of their policies for ambiguities, and to address any existing ambiguities towards clearer and more enforceable policy documents. The next section provides the dissertation structure.

1.11. Dissertation structure

The structure of the dissertation is outlined in Figure 1.2.

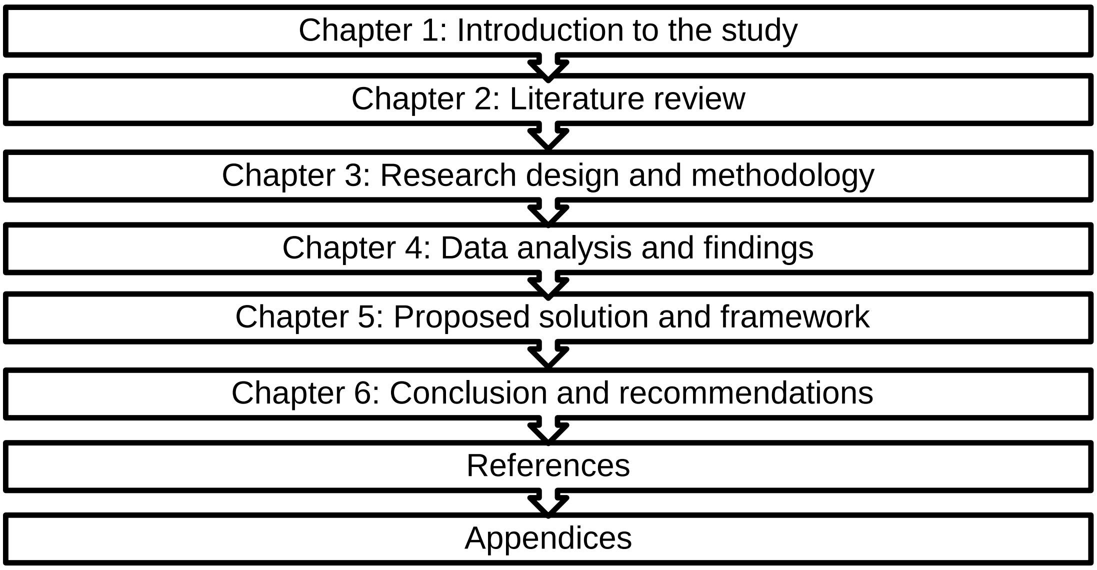

Chapter 1: Introduction to the study
Chapter 2: Literature review
Chapter 3: Research design and methodology
Chapter 4: Data analysis and findings
Chapter 5: Proposed solution and framework
Chapter 6: Conclusion and recommendations
References
Appendices

Figure 1.2: The dissertation structure

Chapter 1 provides the introduction and background of the study, the research problem, questions, objectives, limitations and the significance of the study.

Chapter 2 presents the literature review on InfoSec policies, ambiguity and the higher education context.

Chapter 3 provides the research methodology used for this research project, including the research strategy, design and data-collection and analysis techniques.

Chapter 4 discusses the research results from the data analysis and the interpretation of the findings.

Chapter 5 provides a discussion of the proposed framework for addressing the InfoSec policy ambiguity problem.

Chapter 6, the last chapter, provides the conclusion and recommendations.

The study concludes with a number of appendices.

1.12. Chapter summary

This chapter discussed the research background, problem statement, aims and objectives. It highlighted the significance of the study and defined the research questions as well as the assumptions and limitations.

The study focus area was introduced, the details of the problem were stated, and significance of the study presented to justify the need for this research to be conducted. The research methodology was noted to guide the reader on the path that the researcher took on the research journey.

The next chapter presents the literature review conducted to develop a perspective on the current state of InfoSec, ambiguity, the higher education context and InfoSec policy research areas to inform the research process undertaken.

Chapter 2
Literature review

2.1. Introduction

The previous chapter provided the introduction and background to the study, as well as an overview of the chapters that follow. The research problem and objectives were also presented in the chapter 1. This chapter presents the literature review of the reviewed academic literature relevant to the research objectives and questions of the study. The following research objectives have been addressed in this chapter:

RO1: Explore the literature on InfoSec policies;
RO2: Identify the main problems facing InfoSec policy compliance;
RO3: Identify the main problems relating to ambiguity within InfoSec policies;

The following section explores and presents the academic literature on InfoSec policies.

2.2. Information security policies

The InfoSec policy is often presented to system users at employment induction training or when they are issued with access to institutional information resources. For instance, a system user may be presented with the InfoSec policy when the ICT department issues him or her with a workstation or laptop computer. The system user needs to have accepted the InfoSec policy before institutional information system access can be granted.

Similarly, for students, the InfoSec policy could be presented to the student at registration for their studies. The student would have to accept the InfoSec policy before they could continue and complete the registration process for their studies. Subsequently, some system users sign the InfoSec policy only as a formality in order to receive access to and use the institutional ICT resources, and not because they necessarily understood said policy (Whitman & Mattord, 2012).

User InfoSec policies are those that are read and applied by ICT system users in the form of written documents, while system policies are those applied in the ICT systems in the form of system configurations. The user InfoSec policy is hereafter referred to simply as the InfoSec policy. The InfoSec policy document is used as a security control measure to preserve the confidentiality, integrity and authenticity of institutional and user information by outlining what the institution deems acceptable use of its ICT resources (Whitman & Mattord, 2012).

The effectiveness of information system's security can be achieved through promoting adequate InfoSec behaviour and constraining unacceptable information behaviour among employees in the organisation (Woodhouse, 2007). Lindup (1995) presents four types of security policies: the system security policy, the product security policy, the community security policy and the corporate InfoSec policy.

This research focused on corporate InfoSec policies in the higher education institutional context. These are generally specified and documented in natural language. Do Amaral, Bazilio, Da Silva, Rademaker & Haeusler (2006), state that an InfoSec policy defines the actions to be taken in order to achieve the security control objectives for the organisations' desired level of security.

2.3. The information security policy and higher education

The higher education space has taken considerable interest in using ICT for teaching and learning. A pedagogical shift has taken place where teaching and learning activities have moved from classroom-based to online platforms. Online platforms are referred to as online learning tools, electronic learning (e-learning) platforms and online courseware. There are even free platforms called mobile open online courseware. Technology use has evolved from pen and paper, chalkboard, transparency projectors, overhead projectors and interactive white boards to e-learning based on electronic tools for teaching and learning (Adibi, 2010; Carter, 1996).

The growing need for online learning requires of higher education institutions to use technology and media in the delivery of learning content. Learning is a social process that requires on-demand and online delivery of study content (Harasim, 2002; Swan & Shea, 2005). It was this major ICT adoption by higher education institutions that led the researcher to undertake this study: With the vast technology use for day-to-day teaching and learning came the challenge of securing tuition content online. Tuition content includes student and staff personal information, financial information and student grades (Buthelezi & Mujinga, 2013).

The sensitive nature of tuition content, demands that there should be documented rules and guidelines to govern how this content is accessed, used and stored for secure institutional use of technology (Doherty, Anastasakis & Fulford, 2009; Knapp, Morris, Marshall & Byrd, 2009). Even within the academic space, InfoSec policies and guidelines have been established to accomplish this governance aspect (Soomro, Shah & Ahmed, 2016). InfoSec policies are often documented in ambiguity-prone natural language (Parkin, Van Moorsel & Coles, 2009). The presence of ambiguity could lead to reduced clarity, which could lead

InfoSec policy users to incorrectly executing policy statements, thereby making it difficult to comply with the unclear policies.

The move to an online pedagogy of teaching and learning has also raised user expectations for just-in-time (available around the clock) and just-in-context (students choosing only what interests them) learning, where students want access to the learning materials as and when they need to. According to the findings of prior research, as documented by Lan and Sie (2010), the use of mobile devices to support learning activities has been reported to be beneficial because it encourages learner-to-learner interaction, the same interaction which was reported by Moore and Kearsley (2005) to be motivating and stimulating for learners. This view is supported by Richardson and Swan (2003), who assert that this interaction is critical in learning.

Education has been viewed as a social practice, and learners often use mobile devices for social networking per social learning theory, it follows that mobile devices should be capable of being used as learning tools to support online learning. Social learning theory further perceives learning to take place during social interactions in a community with similar interests (Wenger, 2000). Therefore, by virtue of social networks and discussion forums being social environments, learning should take place on this platform as well.

2.3.1. Human infrastructure

The shift from traditional teaching and learning to ODL brings about a number of challenges for both the student and the institution. At the forefront is the need to train instructors and prepare them for the new way of teaching and learning. That way, they will be better equipped to utilise the infrastructure and assist students in ODL. Hutchins (2003) found that an instructor’s behaviour determines the success of the online learning model, as there are significant differences between the behaviour of online instructors and classroom instructors. This suggests that instructors need to be prepared for online learning delivery, mostly through training in ways of interacting with students through online tools.

2.3.2. Information and communications technology infrastructure

Technological infrastructure refers to all the aspects of ICT facilities that need to be in place for the introduction of ICT in the classroom; this includes ICT devices and networks. Schools need to have proper facilities such as computers with a functional operating system and connected to the internet through faster and usable bandwidth speeds that allow communication with reasonable speeds. The virtual learning environment, also known as the e-learning platform or learning management system, is a set of learning and teaching tools such as discussions, electronic documents and learning units usually provided through a web portal (Van Raaij & Schepers, 2008).

E-learning platforms are becoming an integral part of the teaching and learning process (Pituch & Lee, 2006), but the main problem in developing countries is the high cost and limited bandwidth. Schools are affected most because they have limited financial resources. At the core of online learning is the internet, as it is the delivery medium of online content (Zhang & Nunamaker, 2003). Most of the online content delivery services such as video and audio streaming or playback require high-speed internet compared to browsing (Liu, Guo & Liang, 2008; Wu, Hou, Zhu, Zhang & Peha, 2001). Internet coverage and e-learning implementation in developing economies, especially in Africa, still prove to be a challenge due to lack of infrastructure, particularly broadband (Twinomugisha, 2010).

2.4. Information and communications technology in higher education

Institutions of higher learning provide teaching and learning as the core service to their clients, the students. As discussed, the nature of teaching and learning has since evolved to be a more digitised pedagogy. Higher education institutions have embraced the use of ICT to deliver teaching and learning content to the distantly located student. This trend has seen a proliferation of online learning platform production. This includes off-the-shelf products and some tailor-made products for specific institutions' needs.

Even though teaching and learning have transferred to the online spectrum, its accessibility for the majority of students in developing countries is still a major challenge due to the countries' legacy of internet connectivity problems. Those in rural areas are further constrained by the lack of infrastructure, which introduces a severe obstacle to full adoption of the model by institutions as they are forced to provide alternative modes of teaching and learning to those students still struggling to come on-board the digital highway. In some cases, open and distance learning (ODL) institutions are compelled to provide internet connectivity to students through initiatives such as subsidising bandwidth costs and partnerships with internet service providers and internet café operators.

As a result, ODL institutions end up running two parallel models of content delivery: online and print delivery models. This results in a lack of optimisation and the benefits of online delivery not being fully realised. In the case of situations where e-learning adoption has been embraced to a larger extent, the problem is that of conducting summative assessment.

2.4.1. Electronic learning

E-learning is the use of IT tools for learning purposes (Dabbagh & Kitsantas, 2012). E-learning uses electronic channels for communication and delivery of the teaching and learning content to students. E-learning started as the use of electronic devices such as CDs, DVDs and tapes, which were sent to students and the content opened through a computer, but has now extended to the online mode of delivery (Adibi, 2010).

A typical online learning platform provides tools such as discussion forums, video and audio podcasts and electronic documents. It usually involves two-way communication between students and the institution. According to Smeureanu & Isaila (2008), e-learning qualifies as a type of distance learning, as the educator and the student are often in different locations with asynchronous means of interacting. Craciunas & Elsek (2009) as well as Soomro, Shah, & Ahmed (2016) present the characteristics of e-learning systems as follows: Learning takes place in a virtual class that is coordinated by a facilitator, the content is made available over the internet, learning is a social process, there is activity monitoring of the participants and the environment allows the transfer of knowledge and skills.

Online learning brings about a number of benefits to both the student and the institution. E-learning has shifted the learning process from teacher-focused to learner-centred learning. Previous studies identified the benefit of flexibility to students, as it allows them to collaborate online without the need to rearrange their schedule (Petrides, 2002; Schrum, 2002; Vonderwell, 2003), especially for those students studying part-time and working full-time. Such flexibility is not available in residential institutions. The convenience of choosing the most suitable time to engage with online learning tools is another strength reported by students (Ke & Kwak, 2012).

2.5. Why e-learning requires security

The higher education space has taken much interest in technology as a teaching tool. There has been a drive to be innovative in delivering tuition. With the vast technology use come InfoSec risks and the need to document InfoSec policies and guidelines for secure technology use. There is a great need for securing e-learning systems to ensure that they are not compromised. Securing these systems is also required to gain user confidence in the validity of the online qualification offered.

To secure the e-assessment system, the following, per Marais (2006), have to be addressed: authenticity of the candidate has to be guaranteed, the e-assessment environment has to be monitored, the e-assessment integrity has to be upheld in order to deter electronic corruption, software glitches have to be avoided by performing periodic system maintenance and user privacy and confidentiality have to be ensured in order to gain user confidence in the system. Ensuring the security of an e-learning system is no easy task, and requires the protection of the content, services and personal data for external and internal users, including system administrators, as advocated by Defta (2011).

In the e-learning pedagogy, the tuition content is delivered using the internet, intranet or extranet as a medium (Soomro, Shah, & Ahmed, 2016). The following security concerns affect e-learning by virtue of using the internet as a medium: confidentiality, integrity, availability of information, authorisation, authentication and non-repudiation (Defta, 2011; Graf, 2002). The security concerns coincide with the main pillars of InfoSec, which are confidentiality, integrity and availability of information. Other InfoSec concepts that are to be considered are authorisation, authentication and non-repudiation.

The above principles need to be addressed for the design and implementation of a secure and usable e-learning and assessment system. The security of e-learning platforms has to be considered at system implementation to build controls into it, as well as at the user training phase, to include user e-learning security awareness training. The security awareness training content should be made available to all users of the e-learning system when the system is introduced to them. This can be in the form of computer-based training or self-help documents.

When the users become aware of the security features on the e-learning system, it could improve their confidence in the system and their willingness to accept and use it. Putting security measures in place for an e-learning system is referred to as e-learning security, which is essential to establish e-learning as a trusted tuition medium (Defta, 2011). The security concerns identified to be relevant to this research are the accountability, confidentiality, integrity, availability, non-repudiation and authenticity of e-learning, as follows:

Accountability: Accountability is essential to maintain a good working relationship between the e-learning institution and its students. Both the student and the institution (including employees) have to be held accountable for their conduct on the e-learning platforms. This means that the actions performed in one’s profile will be directly associated with the user and therefore this would be expected to encourage users to protect their profiles and act with integrity. Consequently, the accountability factor would entail placing the security responsibility in the hands of the users and empowering them to secure the e-learning system. Acceptable use policies should be presented to the users at first use to ensure compliance with what is acceptable behaviour when using the e-learning system.

Confidentiality: E-learning material needs to be made available only to authorised users and the system should provide un-spoofable security mechanisms. Confidentiality protects against unauthorised access and distribution of an institution's learning material, as this needs to be made available to enrolled students. Confidentiality is particularly important for e-assessment, as timing of the assessment release is of vital importance and only authorised students should have access to the e-assessment for a specified period of time. Confidentiality also ensures that user data are kept confidential and are not available to unauthorised users; such data include personal information and assessment results.

Integrity: Integrity addresses the need for the information not to be modified by unauthorised users, ensuring that information integrity is preserved. Only authorised users of the e-learning system should be allowed to modify or delete the learning material. The system should allocate appropriate rights to students and online facilitators. Modification of e-learning material should be performed by legitimate and authorised system users. Such information includes learning material and assessment results. The integrity concern is also considered from the perspective of conducting summative assessments, where students are assessed remotely and with no proper mechanisms to identify the assessment candidate.

Availability: One of the main drawcards of the e-learning model is its availability twenty-four seven. The availability of an e-learning web portal is important and the system should be protected from availability security threats such as denial of service and distributed denial of service. The University of South Africa (Unisa) has students from all over the globe and to accommodate different time zones, the system should allow students to log onto the system 24 hours a day.

ODL students often partake in study and work at the same time, hence continuous system availability facilitates easier learning and allows students a flexible study and work schedule. The availability aspect extends to system availability when the students need to access it. There are chances that the system could become overloaded during peak usage times. The system could also be unavailable during its maintenance and update periods. Therefore, prior communication of scheduled system interruptions is sent to the students so that they are aware and can prepare for system downtime.

Non-repudiation: Non-repudiation ensures that system users do not refute actions they performed on the system. An e-learning system should provide integrity of the source of actions and ensure that messages or actions are not modified in transit. This is usually achieved through mechanisms such as digital signatures using public key infrastructure.

Authenticity: Authenticity specifically pertains to ensuring the identities of the parties involved in a communication, thereby avoiding man-in-the-middle and identity theft attacks. In e-learning, this usually involves a user and the e-learning server, so as to avoid leakage of confidential information to the wrong parties. This is of particular importance to e-assessments, where the identity of a remote user is an integral part of the whole model (Rowe, 2004).

Violation of authenticity brings into question the quality of a qualification being offered online, and ultimately the reputation of the institution is affected. This problem has resulted in a number of studies attempting to find a solution to positively identifying the assessment candidate when assessment is conducted in an unsupervised environment (Apampa, 2008; Furnell, 1998; Graf, 2002; Marais, 2006; Rowe, 2004). For instance, Church and Oliver

(2011) propose a safe and secure solution for remote supervision of a video-based examination with easily available hardware and software tools.

Privacy: Privacy is concerned with the collected information being used only for its intended purpose. In the context of e-learning, privacy ensures a student's ability to maintain a 'personal space' within which the student can control the conditions under which personal information is shared with others (El-Khatib, Korba & Xu, 2003). This information includes students' personal information and contact details, as well as collected identification information such as personal information, login details and biometric information (Apampa, Wills & Argles, 2010). Violations include using contact information for non-academic purposes. Usually the importance of privacy is recognised only after it has been breached.

2.6. Barriers to information security policy compliance

InfoSec policy compliance is a well-researched area and InfoSec policy non-compliance has been attributed to the following reasons as barriers to compliance, as depicted in Figure 2.1:

- *Lack of management support for information security:*

Prior research cites management support as one of the most important components of effective InfoSec management (Doherty, Anastasakis & Fulford, 2009; Padayachee, 2012; Whitman & Mattord, 2012). Hu, Dinev, Hart & Cooke (2012) found that the participation and commitment of top management in terms of InfoSec management had a significant impact on employee attitudes towards InfoSec policy compliance.

- *Organisational culture:*

Organisational culture can affect user compliance with the InfoSec policy, based on what is deemed as acceptable behaviour among fellow employees. Siponen & Vance (2010) refer to this phenomenon as an ‘appeal to higher loyalties’. A security-aware culture would encourage InfoSec policy compliance (Da Veiga & Eloff, 2010). Organisations should cultivate an InfoSec-receptive culture (Thomson, Von Solms & Louw, 2006).

- *Information security policy awareness and training:*

Some policy users have been reported to have perceived the InfoSec policy to be a nuisance by restricting their freedom to use the systems (Dagada & Eloff, 2013). Educating users on their InfoSec roles leads to increased policy awareness, which has been advocated to increase compliance (Siponen, Mahmood & Pahnila, 2014).

- *Human aspects of information security:*

It has often been said that the weakness of any security system are the people using the policies (Parsons, McCormac, Butavicius, Pattinson & Jerram, 2014). Much of prior research has focused on measuring compliance levels and evaluating the human aspects of compliance. These human aspects of compliance have been extensively evaluated based on theories from the field of psychology and criminology, such as the theory of planned behaviour, deterrence theory as well as protection motivation theory (Ifinedo, 2012).

- *Information security policy clarity:*

The words ‘lack of policy clarity’ have often been used to refer to ambiguity in policies. The InfoSec policies have been reported to be too long and ambiguous. The existence of ambiguity has been largely discussed in the requirements specification field of research. Although policy ambiguity has been suggested as a barrier to policy compliance, the researcher did not find much research that has been conducted to review actual InfoSec policy documents for possible ambiguities that might lead users to misinterpret the policy.

An overview of the different barriers to InfoSec policy compliance have been presented as a conceptual framework in Figure 2.1.

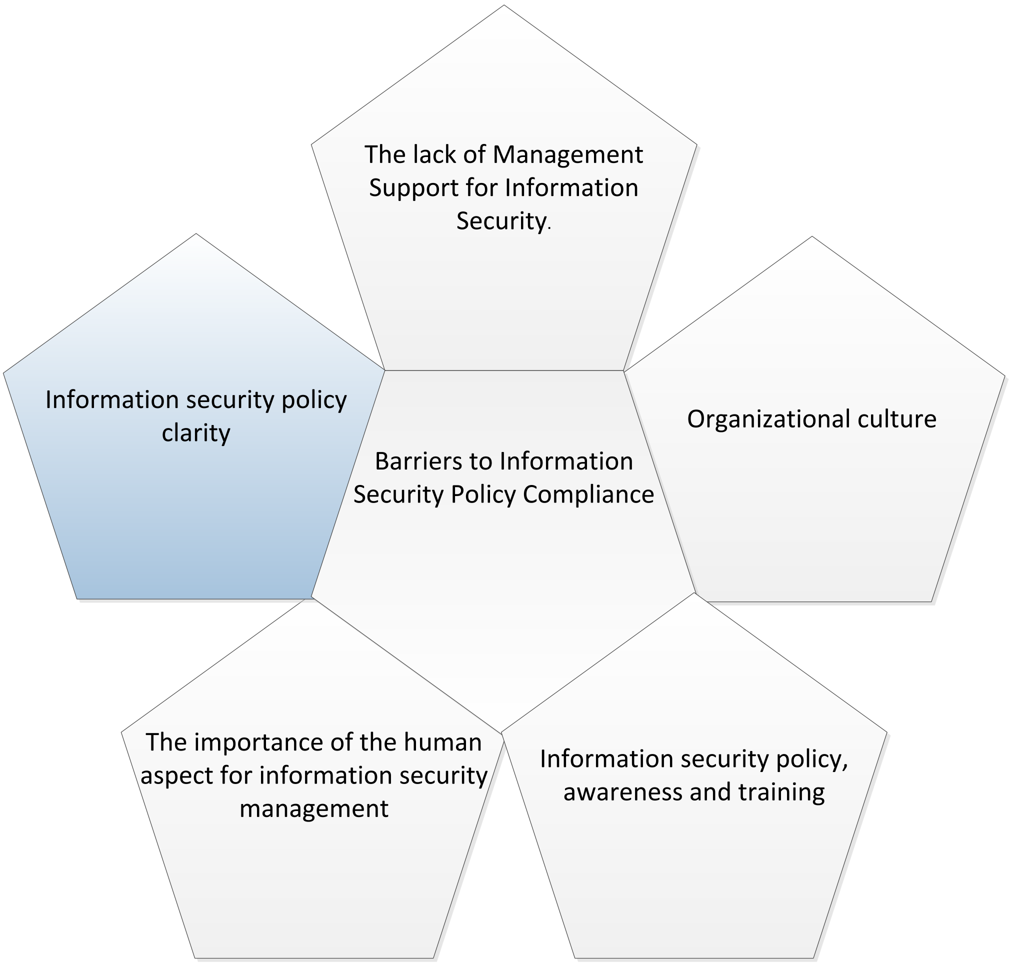

The lack of Management Support for Information Security.
Information security policy clarity
Organizational culture
Barriers to Information Security Policy Compliance
The importance of the human aspect for information security management
Information security policy, awareness and training

Figure 2.1: Conceptual framework: Barriers to Information security policy compliance (Synthesised by researcher)

Rees et al. (2003) point out that there is a challenge in keeping InfoSec policies consistent; while Doherty, Anastasakis & Fulford (2009) report that an effective InfoSec policy document can reduce security breaches. The focus of this study was therefore on InfoSec policy clarity, as depicted in the shaded part of Figure 2.1 on the left hand side, which reflects the conceptual framework for the study.

InfoSec policy clarity as a policy compliance barrier could have a negative ripple effect on all the other barriers regardless of how well they have been addressed. Therefore, there should be more focus on increasing policy clarity and reducing ambiguity. No matter how much top management commitment or participation is provided to InfoSec management, an unclear policy could just as well lead the same top management to non-compliance by misinterpretation. The same goes for changing the organisational culture and increasing InfoSec policy awareness and training.

The presence of ambiguity within the InfoSec policy document could render these efforts futile. Therefore, it is becoming essential to investigate the problem of ambiguity in order to get a better understanding and subsequently address the problem. The next section discusses the different types of ambiguity from academic literature.

2.7. Types of ambiguity

Ambiguity occurs when words or even images have more than one possible interpretation in terms of their meaning (Rees et al., 2003). The term 'ambiguity' was used to refer to a single word with multiple meanings (Jayadianti, Nugroho, Santosa, 2014). The multiple meanings reduce clarity of the message delivered. Ambiguity can be beneficial when used intentionally in art, literature, humour and poetry. It can be enchanting in literature, as it allows one to use one's imagination to create meaning and therefore makes the literature captivating and enchanting (Bucaria, 2004). One example of beneficial ambiguity is per the below quote (McCloskey in Ryan, 2014): "I know that you believe you understand what you think I said, but I'm not sure you realise that what you heard is not what I meant".

Although ambiguity can be beneficial, it can also be a limitation in instances where the reader or listener in communication has to make decisions based on the message communicated to him or her, but the message happens to be an ambiguous statement. This would reduce the level of decision precision, as the statement would be prone to misinterpretation. Kamp and Uwe (1993) draw attention to the idea that languages are for message exchange and sharing meaning. They reflect this phenomenon in yet another way by using a communication analogy, suggesting the speakers should clearly articulate or verbalise their thoughts and the hearers should discern meaning from the words that they have heard.

This is applicable to speaking or writing as well as hearing or reading. Kamp and Uwe (1993) further suggest that communicators should find the words that are relevant to the content or message to be conveyed to ensure that the recipient can identify the content from the received words in a message. Computational linguistics literature refers to six kinds of ambiguity as follows:

Lexical ambiguity

This occurs when multiple meanings of one word cause a single word or a string of words to be interpreted in different ways, because some words have more than one meaning (Chierchia & McConnell-Ginet, 1990); for example, the word ‘bank’ can refer to a slope side of a river or a business establishment.

Structural ambiguity

This is also called syntactic ambiguity or grammatical ambiguity, and occurs in sentences where the meaning of each word is clear, but the words of a sentence are related to one another in various ways (Empson, 2004); for example, “She saw a man with binoculars”.

Does it mean that she looked through binoculars and saw a man, or does it mean she saw a man, and he had binoculars with him?

Semantic ambiguity

This occurs when even after the syntax and the meanings of the individual words have been resolved, there are two ways of reading the sentence. One indicator signifies more than one concept (Abbott, 1997); for example, “John kissed his wife, and so did Sam” (Sam kissed John’s wife or his own?)

Anaphoric ambiguity

This type of ambiguity occurs when a phrase or word refers to something previously mentioned, but there is more than one possibility; for example, “Margaret invited Susan for a visit, and she gave her a good lunch” (she = Margaret; her = Susan); “Margaret invited Susan for a visit, but she told her she had to go to work” (she = Susan; her = Margaret.)

Durational ambiguity

In this form of ambiguity, the duration unit of analysis is unknown but consequential (Abbott, 1997). For example, “One should look left, then right for a reasonable period before crossing the road”.

Omissions/Null pointer

Ambiguity can also occur as a result of a statement/guideline or section that has been omitted from a policy document, in other words, ambiguity by omission (Abbott, 1997).

The above ambiguity types were used to derive the themes for the content analysis coding scheme listed in Table 3.3 in Chapter 3. InfoSec policy non-compliance has been studied comprehensively. On the other hand, to the knowledge of the researcher there is little available research related to the wording of InfoSec policies and the presence of ambiguity. The available research has focused on software requirements, system security policies and password policy.

2.7.1. The ambiguity problem occurrences

Before InfoSec policy users can execute the policy statements, they first have to interpret such statements before making the decision on which statement to execute and how to execute it. It is in this interpretation process where policy statements can be misinterpreted and wrongfully executed in the presence of ambiguity.

Below are some of the ambiguities that were noted in InfoSec policy details. These ambiguities are also reported by Kolkowska & Dhillon, (2013), where an InfoSec policy description was inconsistent due to the conflict in functional rules and where several security objectives might have been contradicting each other, a view supported by Doherty, Anastasakis & Fulford (2009).

During the content analysis of the *policy document OP2*, a document collected online. While working towards deriving and establishing the final content analysis themes. It was noted in this document's access control section that:

> "[u]sers should have unique combinations of usernames and passwords" (Hostland et al., 2010:21).

However, the requirement does not provide details of the username or password structure to ensure uniqueness. This requirement statement is open-ended as compared to its counterpart in the InfoSec regarding physical conditions, which states that:

> "[a]ll external doors and windows must be closed and locked at the end of the work day" (Hostland et al., 2010:16).

The above requirements come from the same InfoSec best practice document, and contain different levels of detail. In the same way as the comparison in the previous paragraph, there is a level of assumed reader implicit knowledge in the first requirement and the latter is explicitly stated in clear terms. This is an example of some requirements being vaguely stated and others in specific elaborate details in the same policy document, which leaves the interpretation to the background knowledge of the reader and causes discrepancies.

Further examples of vague specifications contrasted with elaborate ones are documented below as noted from the Princeton University Information Security Policy (Princeton University, 2009):

Example of vagueness: "Users should lock or log off their computers before leaving them unattended" (Princeton University, 2009:15). It appears as though the users are encouraged to leave their computers unattended. Also, it is not entirely clear when a computer is not attended to – user still in visual range of the computer, or user left the room.

Elaborate example: "Tangible records (paper documents, microfilm, etc.) containing Confidential or Highly Confidential information must be:

- stored in a locked cabinet or drawer when not in use with access limited to authorized individuals, and

- physically shredded/destroyed when no longer needed" (Princeton University, 2009:16).

The above are detailed situations and associated actions.

Example of vagueness: "Computers should be configured to 'time out' after no more than 20 minutes of inactivity" (Princeton University, 2009:15). After how many minutes of inactivity should the computers be configured to time out? It appears as though any number from 1 to 20 minutes.

Elaborate example**:** "Ensure that any system is configured to keep a record of:

- Who attempted to log into the system (successfully and unsuccessfully) and when,
- When they logged out,
- Administrative activity performed,
- Unsuccessful attempts to access confidential and highly confidential files" (Princeton University, 2009:15).

The requirements are clear on what activities should be logged.

Generally, some of the documents that are faced with the ambiguity problem include, but are not limited to, software requirements specification documents, system security policies, password policies and user information security policies.

2.7.1.1. Software requirements specification

Sommerville (2013) reports on the ambiguity of natural language in the field of software engineering, where there were problems noted when natural language was used for software requirements specifications. Lack of requirement clarity was identified, which affected the precision of the requirements. Requirements were confusing in a way that resulted in functional and non-functional requirements being confused, where functional requirements were mistaken for non-functional requirements and vice versa.

Somerville (2004) also noted requirements amalgamation where several different requirements could have been expressed as one requirement. The researcher postulates that these challenges are not unique to software requirements specifications and could also be extended to the InfoSec space, where ambiguity can be a problem in the specification and documentation of InfoSec policies.

2.7.1.2. System security policy

In the case of system security policy research, software solutions were recommended to automate the process of ambiguity detection and resolution (Singh, Ramakrishnan, Ramakrishnan, Stoller & Warren, 2007). The study by Jayadianti, Nugroho, Santosa (2014) was conducted in order to address the ambiguity that could arise in instances where the human and the computer or one computer and another have different understandings of the same terms, i.e. where terms can generate ambiguity. Jayadianti, Nugroho, Santosa (2014) reason that naturally, computers are better than humans in performing calculations of complex numerical values as well as in remembering things, but not in integrating and sharing knowledge from different sources with different semantics, vocabulary and contexts (Jayadianti, Nugroho, Santosa, 2014).

People are better at integrating knowledge because they can consult, discuss and debate with one another to arrive at a common solution to a problem (Jayadianti, Nugroho, Santosa, 2014). Although humans have been regarded to be better than computers in dealing with ambiguity in their day-to-day communication, they are not exempted from the problem of misinterpreting ambiguous terms (Jayadianti, Nugroho, Santosa, 2014).

2.7.1.3.Password policy

The work of Tryfonas & Askoxylakis (2015) focused on password policy ambiguity. Tryfonas & Askoxylakis (2015) conducted a study in which they developed methods and tools for studying and clarifying system password policy statements in order to reason about the relationship between the system password policy and the system user behaviour. The authors found there were ambiguities present in password policies. These ambiguities could alter user behaviour in the form of policy misinterpretation, and such misinterpretation could lead to policy non-compliance by users (Tryfonas & Askoxylakis, 2015).

Furnell (2007) conducted a study in which he reviewed the password management guideline sections of ten website policies and found that password policies that ignored human factors could lead to poor security. There is an emerging importance placed on the relevance of policy content affecting user compliance. Mannan & Oorschot (2008) conducted a survey among online banking users, and found that user practices were not in line with the bank-provided guidelines.

2.7.1.4. User information security policy

InfoSec policy users are subjected to multiple, different policies at home and at work (Doherty, Anastasakis & Fulford, 2009; Tryfonas & Askoxylakis, 2015; Whitman & Mattord, 2012). Some of the policies that could govern a typical InfoSec policy user include policies for access to and handling of corporate documents, personal financial information, online shopping content, social media content, personal medical records as well as smart fitness device content. According to Tryfonas & Askoxylakis (2015), ambiguities contained in policies and user misinterpretation of the password policies could have a major, negative impact on an organisation's InfoSec compliance.

The password policy is often documented as a section within the InfoSec policy document. Therefore, the applicability of the findings by Tryfonas & Askoxylakis (2015) could be validated against the full InfoSec policy document. Similarly, the presence of ambiguity in the full InfoSec policy could bear negative consequences for user compliance. This study explored whether it is the policy documents that pose a compliance problem by containing ambiguities that could lead the users to executing the policy statements incorrectly as a result of possible policy misinterpretations.

Literature has suggested some solutions to ambiguity as it occurs in requirements specification documents. The next section discusses some suggested solutions.

2.7.2. Proposed solutions to ambiguity

Hinchey & Bowen, (1996), Parkin, Van Moorsel & Coles, (2009), and Tjong, (2013), have suggested the following strategies to reduce ambiguity in requirements specification, and they could be tested for applicability to reduce ambiguity in InfoSec policies:

- Ontologies
- Automated disambiguation tools such as SREE (Synthesized Requirements Engineering Environment)
- Manual analysis
- Formal methods.

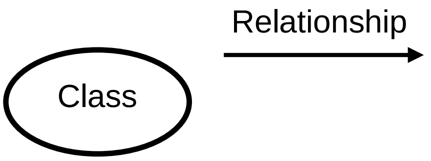
For the purpose of this study, manual analysis and formal methods were used and tested as possible solutions to derive the frameworks for resolving ambiguity in InfoSec policy documents. Formal methods have previously been reported to have been applied reduce ambiguity in natural language text (Hinchey, Bowen & Rouff, 2006; Do Amaral, Bazilio, Da Silva, Rademaker & Haeusler, 2006).

2.7.2.1.Ontologies

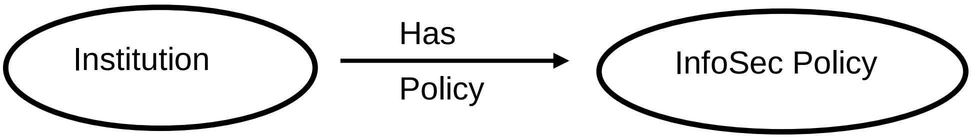
An ontology is a model to represent knowledge (Guarino & Giaretta, 1995). It consists of a set of concepts in a domain, as well as relationships between these concepts (Guarino & Welty, 2004). An ontology depicts knowledge as a model.

Parkin, Van Moorsel & Coles (2009) developed an InfoSec ontology to better understand human behavioural factors in the InfoSec space. Things are described as classes in relation to one another.

Ontological notation:



For example:



Ontologies have also been used for the speech recognition aspect of intelligent applications as a formal knowledge representation; for example, the Seri tool used by the Apple iPhone, where a phone user dictates to the phone what actions the phone should take, such as “Call John Doe”, after which the phone processes the instructions.

Some of the ontology-related research was conducted in the area of machine learning. Ontologies in machine learning have been used to manage the knowledge that the computers acquire and reduce the probability of the same terms being understood differently by different computer machines (Guarino & Welty, 2004; Parkin, Van Moorsel & Coles, 2009). The ontologies were also applied by Jayadianti, Nugroho, Santosa (2014) as a technique for representing specific knowledge that is saved in each computer and to find the correspondences between the concepts used in those ontologies. Since this research opted for the use of manual techniques and formal methods, further discussion of ontologies is beyond the scope of this dissertation.

2.7.2.2.Automated tools

Jayadianti, Nugroho, Santosa (2014) reason that computers are naturally better than humans in performing calculations of complex numerical values as well as in remembering things, but not in integrating and sharing knowledge from different sources with different semantics, vocabulary and contexts (Jayadianti, Nugroho, Santosa, 2014). People are better at integrating knowledge because they can consult, discuss, debate with each other to arrive at a common solution to a problem (Jayadianti, Nugroho, Santosa, 2014).

Although people have been regarded to be better than computers in dealing with ambiguity in their day-to-day communication, they are not exempted from the problem of misinterpreting ambiguous terms (Jayadianti, Nugroho, Santosa, 2014).

The existence of ambiguity has been largely discussed in the requirements specification field of research, for example "When a user fails to authenticate after a number of times, send a notification to IT" (Jayadianti, Nugroho, Santosa, 2014). In this example, it is not clear how many times "a number of times" is. The programmer cannot simply set a random limit such as a thousand times in the case of automation.

Many automatic tools for ambiguity detection have been investigated in literature. These tools were used to detect ambiguity in requirements specifications that were expressed in a natural language (Tjong, 2013). The automated ambiguity detection tools were parsers- and parts-of-speech-identifier-based, such that they identify ambiguity by labelling each word as a part of speech in order to find the ambiguity in the requirements specifications. The tools were commonly referred to as ambiguity finding tools (AFT).

Wills, Chantree & De Roeck (2008) designed a prototype AFT called SREE. They tested the prototype and found that it did not achieve its goals. SREE was built mainly for use with requirements analysis. Most literature on ambiguity in the information systems and computer science fields has focused on tool-assisted ambiguity detection and disambiguation using AFTs.

The use of such tools still required a manual ambiguity search process, which renders them imperfect on real natural language text (Tjong, 2013). Therefore, the tools would not be a practical solution for disambiguating InfoSec policy documents, if a manual ambiguity search would be necessary in addition to using an AFT (Gleich, Creighton & Kof, 2010).

The AFTs were built with a corpus of specific domain knowledge from Software Requirements and Software development. A tool corpus for InfoSec policy knowledge would have to be built, populated and tested with multiple iterations in order to include an exhaustive list of relevant indicators from InfoSec. The InfoSec domain corpus would have to use prototypes to evolve and further develop the corpus detail, as well as tool recall and precision.

2.7.2.3.Manual analysis

In their 2008 study, Kiyavistkaya, Zeni, Mich & Berry (2008) used 17 requirements specification statements to conduct a manual ambiguity identification process in order to identify ambiguities in requirements specification documents that could have been missed by a LOLITA-based automation tool, which they refer to as T1. Their final output consisted of tool analysis as well as a manual analysis, which they refer to as the inspection approach. Their results indicated that manual analysis proved to be more effective in identifying ambiguities.

For this research, there was no tool use in order to facilitate the replication of the process and techniques proposed in this research work , because the tool requires some technical knowledge to set it up, which some of the InfoSec policy writers might not possess. However, the manual analysis was presented with clear instructions for the process that was followed. This research followed a manual analysis process similar to the manual analysis of Kiyavistkaya et al. (2008), which was applied to the InfoSec policy documents. For this research, formal methods were tested in providing clarity and reducing ambiguity. The next section discusses formal methods.

2.7.2.4.Formal methods

Formalisms, also referred to as formal methods, are mathematical ways of representing information (Hinchey & Bowen, 1996). There are a variety of mathematical modelling techniques that are often applied to computer systems design, system specification, program verification, specification analysis and proof (Hinchey, Bowen & Rouff, 2006). These formalisms are mathematical and formal logic approaches to software and system development, as they exploit the power of mathematical notation and proofs (Hinchey & Bowen, 1996).

Formalisms are sometimes said to guarantee that software is perfect, work by proving that programs are correct, involve complex mathematics, increase the cost of development, are incomprehensible to clients and nobody uses them for real projects (Geyer-Schulz & Chuck Dyer, 2004). However, since such software has to run in the real-world, these are some of the myths about formal methods (Rademaker & Haeusler, 2006).

It has been suggested that formal methods could improve InfoSec policies and render them more precise and comprehensible (Hinchey, Bowen & Rouff, 2006). Do Amaral, Bazilio, Da Silva, Rademaker & Haeusler (2006:20), put it in this way: “Formalized policies are more precise than their informal counterparts; in what concerns communication”. These authors recommend the use of formalisation to extract the semantics of the intended action statements from security policies. This was consistent with the intended results for this research, using a formalism that is user-friendly and enables comprehensibility and ease of implementation by users (Hinchey & Bowen, 1996).

Hinchey, Bowen & Rouff (2006) identified precision, conciseness, abstraction and reasoning as the main benefits of using formal methods in documenting specifications. These benefits were detailed as follows: precision to reduce ambiguity of natural language, conciseness to make the document easier to comprehend, and abstraction and reasoning to facilitate validation of the specification using mathematical reasoning. Meyer (1985) states that he supports the use of formal specifications to complement instead of replacing natural language descriptions.

Hinchey and Bowen (1996) write they have seen the development of formal methods from being used for software specifications in the 1980s to policies in the 2000s. This shows the formal method application improvements made over 20 years. This research aimed to make a contribution to the noted improvements.

This research applied formal methods as possible solution to determine whether formal methods could improve on the InfoSec policies and render them more precise and comprehensible (cf. Hinchey, Bowen & Rouff, 2006).

2.7.2.5. Formal methods use

The use of formal methods has previously focused on the software engineering space; however, their use is slowly progressing to include system security specifications (Hinchey, Bowen & Rouff, 2006). A formal specification is also referred to as a logic; logic can be seen as the study of correct reasoning (McCawley, 1981; Shapiro, 2000), which, according to Almeida, Frade, Pinto, & de Sousa (2011), is a study of the principles of reasoning. Logic reasoning is about situations and constructing arguments about these situations.

A logic or formal specification consists of three aspects, reported by Do Amaral, Bazilio, Da Silva, Rademaker & Haeusler (2006) as:

- *Syntax or logical language:* These include grammatical rules to determine whether sentences are well formed. It is a language in which sentences are expressed each with their own logical symbols with defined and fixed/rigid interpretation, and non-logical ones with flexible, non-fixed interpretations. These symbols can be combined to form well-formed formulas).

- *Semantics:* These are rules for interpreting the sentences in a precise, meaningful way within the domain. It differentiates valid sentences from refutable ones. Semantics is defined in terms of the truth values of sentences using an interpretation function that assigns meaning to the basic concepts within the domain.

- *Proof theory/Inference system:* These are rules for inferring useful information from the specification. These rules support the formalisation of arguments, justifying the validity of sentences.

There are three well-known logics as reported by Almeida et al. (2011). These are propositional logic, first-order logic and higher-order logic. First-order logic is the most commonly used due to its expressiveness and ease of use (Do Amaral, Bazilio, Da Silva, Rademaker & Haeusler, 2006). Meaning in propositional logic is context-independent, unlike natural language, where meaning depends on context. Propositional logic has very limited expressive power. It has been referred to as a weak language, because it is hard to identify 'individuals' (e.g. Mary, 3) and one cannot use propositional logic to directly talk about properties of individuals or relations between individuals (e.g. "Bill is tall").

First-order logic (abbreviated FOL; also referred to as first-order predicate calculus [FOPC]) is expressive enough to concisely represent this kind of information. FOL adds relations, variables and quantifiers, e.g.:

- *"Every elephant is grey":* $\forall$ x (elephant(x) $\rightarrow$ grey(x))
- *"There is a white alligator":* $\exists$ x (alligator(x) $\wedge$ white(x))

Propositional logic assumes the world contains facts, whereas FOL (like natural language) assumes the world contains:

- *Objects*: people, houses, numbers, colours, baseball games
- *Relations*: sibling of, larger than, part of, comes between
- *Functions*: parent of, best friend, one more than, plus.

FOL has the following constructs (Do Amaral, Bazilio, Da Silva, Rademaker & Haeusler, 2006):

- Constant
- Variable
- Predicate
- Function
- Connective

- Quantifier

Syntax of FOL: Basic elements

- Constant symbols: King John; 2; University of Johannesburg
- Predicate symbols: Brother; >
- Function symbols: Sqrt; LeftLegOf
- Variable symbols: x; y; a; b;
- Connectives: ¬, ⇒, ∧, ∨, ⇔
- Equality: =
- Quantifiers: ∀, ∃
  - Universal: ∀**x**
  - Existential: ∃**x**
- Punctuation: ( )

2.7.2.6.The use of FOL constructs (quantifier scope)

FOL allows variable arguments. These are quantified in two ways: existentially and universally (Geyer-Schulz & Chuck Dyer, 2004; Do Amaral, Bazilio, Da Silva, Rademaker & Haeusler, 2006).

The universal one is

- ∀x [Expression] - means (for all (x) Expression).
- For example:
  - ∀x [policy(x) => has-owner(x)].
  - The expression in [] is the scope of variable x.
- Existential quantification appears like
  - ∃x [policy(x)] - means (exists (x) such that x is a policy)

- There is at least one x that make policy(x) true.

Switching the order of universal quantifiers *does not* change the meaning:

- $(\forall x)(\forall y)P(x, y) \leftrightarrow (\forall y)(\forall x) P(x, y)$

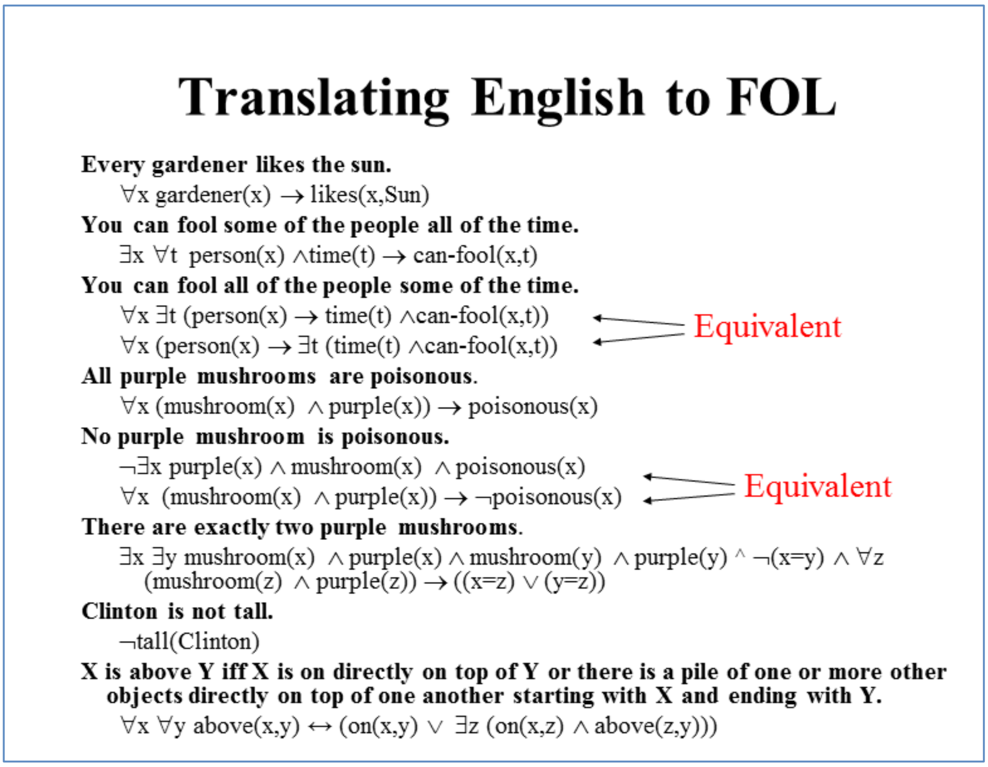
Similarly, you can switch the order of existential quantifiers:

- $(\exists x)(\exists y)P(x, y) \leftrightarrow (\exists y)(\exists x) P(x, y)$

Switching the order of universals and existential *does* change the meaning:

- Everyone likes someone: $(\forall x)(\exists y)$ likes(x, y)
- Someone is liked by everyone: $(\exists y)(\forall x)$ likes(x, y)

Figure 2.2 shows examples of the translation of English natural language (NL) statements to FOL.



Translating English to FOL

Every gardener likes the sun.

$\forall x$ gardener$(x) \rightarrow$ likes(x,Sun)

You can fool some of the people all of the time.

$\exists x\ \forall t$ person$(x) \wedge$time$(t) \rightarrow$ can-fool(x,t)

You can fool all of the people some of the time.

$\forall x\ \exists t$ (person$(x) \rightarrow$ time$(t) \wedge$can-fool(x,t))

$\forall x$ (person$(x) \rightarrow \exists t$ (time$(t) \wedge$can-fool(x,t)))

Equivalent

All purple mushrooms are poisonous.

$\forall x$ (mushroom$(x) \wedge$ purple$(x)) \rightarrow$ poisonous(x)

No purple mushroom is poisonous.

$\neg\exists x$ purple$(x) \wedge$ mushroom$(x) \wedge$ poisonous(x)

$\forall x$ (mushroom$(x) \wedge$ purple$(x)) \rightarrow \neg$poisonous(x)

Equivalent

There are exactly two purple mushrooms.

$\exists x\ \exists y$ mushroom$(x) \wedge$ purple$(x) \wedge$ mushroom$(y) \wedge$ purple(y) ^ $\neg(x=y) \wedge \forall z$ (mushroom$(z) \wedge$ purple$(z)) \rightarrow ((x=z) \vee (y=z))$

Clinton is not tall.

$\neg$tall(Clinton)

X is above Y iff X is on directly on top of Y or there is a pile of one or more other objects directly on top of one another starting with X and ending with Y.

$\forall x\ \forall y$ above$(x,y) \leftrightarrow$ (on$(x,y) \vee \exists z$ (on$(x,z) \wedge$ above(z,y)))

Figure 2.2: First order language translations (Almeida et al., 2011)

Example 2.1

Given an InfoSec policy p, FOL denotes such by saying “For all object p Policy (p)”. Then we are able to reason about this given policy per the below statements.

NL: If a policy is formal, it has no ambiguity
FOL: $[\text{Policy }(p) \land \text{Formal }(p)] \rightarrow \neg\, [\, (\text{Ambiguity }(p)]$

NL: All formal policies have no ambiguity
FOL: $\forall[\text{Policy }(p) \land \text{Formal}(p)] \rightarrow \neg\, [\, (\text{Ambiguity }(p)\,]$

More translation examples from English to FOL:

No documentation language is perfect (two ways)
$\neg\exists x \text{ documentation }(x) \land \text{language }(x) \land \text{perfect }(x)$ $\forall x\, (\text{documentation}(x) \land \text{language }(x)) \rightarrow \neg\text{perfect}(x)$

This research aimed to apply the FOL reasoning to InfoSec policies such that the arguments are valid and can be rigorously defended (cf. Almeida et al., 2011). Formal logic was applied to the InfoSec policies. Broadly speaking a formal logic is a language with rules that determine whether the truth of one sentence can be derived from the truth of other sentences (Almeida et al., 2011). This aspect of logic was useful for the interpretation of InfoSec policies to ensure that the truth of the translated statement is maintained.

2.8. Chapter summary

This chapter presented the literature review conducted on InfoSec policies and higher education research areas to inform the research process. The literature has assisted the researcher to support and counter aspects of the proposed argument and assumptions.

In the next chapter, the research methods and philosophical perspective of the research are presented as well as the research design and methodology applicable to the study. The chapter acts as a point of departure and roadmap for the research journey.

Chapter 3

Research design and methodology

3.1. Introduction

The previous chapter presented the academic literature that relates to the research topic. This chapter presents the research design and methodologies followed in achieving the research objectives set for this study and addressing the research questions, including discussions on how the data was collected and analysed. The structure of this chapter was guided by the sequence of the layers in the structure of the research onion as seen in Figure 3.1 (Saunders, Lewis & Thornhill, 2009).

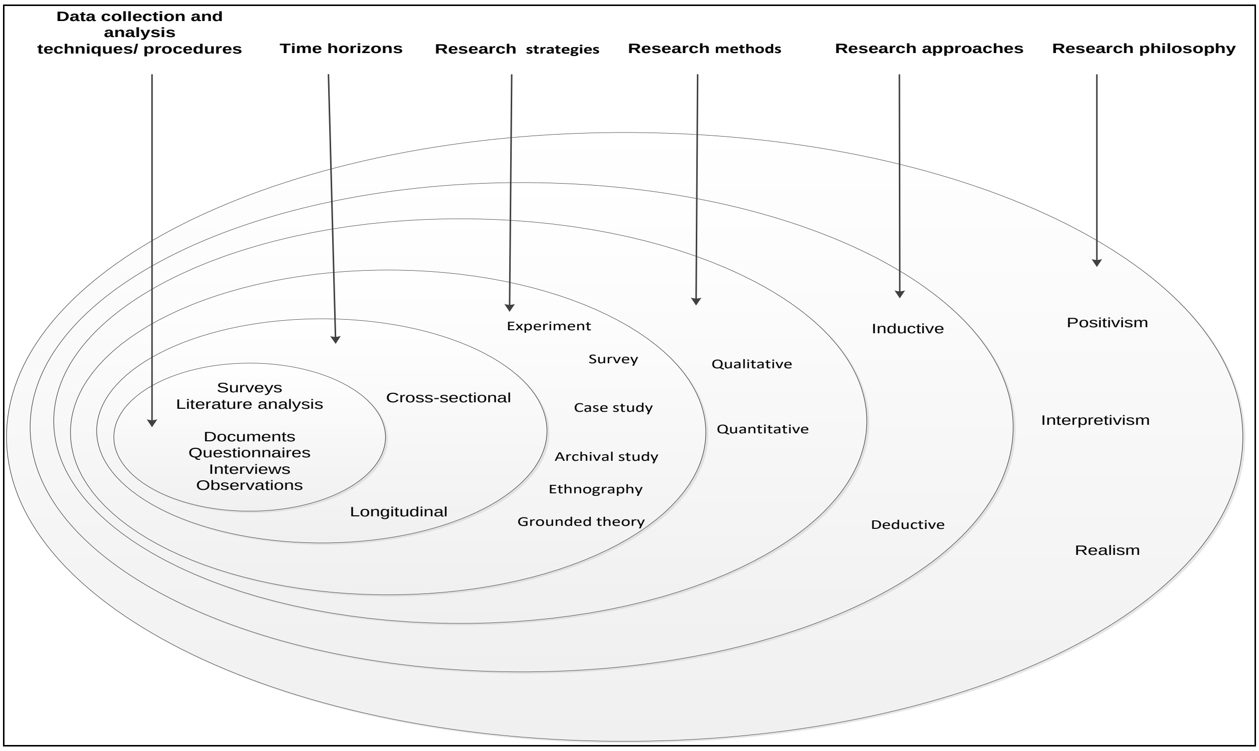


Figure 3.1: The research onion adapted from Saunders, Lewis & Thornhill, (2009)

The research onion was developed by Saunders, Lewis & Thornhill, (2009), to indicate the key stages through which a researcher should pass in order to have an effective research methodology for a research project.

The research methodology discussion in this chapter starts with an overview of the research philosophy in section 3.2, and then the research approach is presented in section 3.3. Followed by an outline of the research methods in Section 3.4, and the research strategies in section 3.5. Thereafter, Section 3.6 presents the research time horizons; Section 3.7 provides the data collection and analysis techniques. And lastly, section 3.8 provides a concluding summary of chapter 3. The next section presents the research philosophy.

3.2. Research philosophy

The research philosophy reflects the researcher's perspective and point of departure for the research, i.e. the nature of knowledge as seen by the researcher (Bryman, 2012). The research philosophy is also referred to as the philosophical paradigm. The research philosophy includes the researcher's ontology, which is his or her belief about reality, and the researcher's epistemology, which is his or her theory of how knowledge is acquired (Wynn & Williams, 2012). Oates (2006) defines ontology as the perception of the world and epistemology as the ways in which we gather knowledge about this world.

There are three main philosophical paradigms that are commonly used to inform the research process, namely positivism, interpretivism and realism as depicted in the research onion per Figure 3.1 (Saunders, Lewis & Thornhill, 2009; Flick, 2011). The epistemologies associated with these philosophical paradigms are empiricism, constructionism and critical realism respectively (Bryman, 2012). The words, "philosophical paradigm", and “epistemology” are often used interchangeably. Krauss (2005) defines epistemology as knowledge about knowledge.

The research philosophies do not compete, but they differ based on the goals of the research project and are chosen based on the best one that might be used to achieve these goals (Goddard & Melville, 2004). The research philosophy is determined by the type of knowledge being investigated and the philosophy will guide the researcher into the relevant research methods (May, 2011).

The associated ontologies refer to the researcher’s views of the nature of reality and these are: For positivism, reality is perceived as objective, external and independent of the social actors (Myers, 2013). In the interpretivist philosophy, the researcher ontology is that reality is subjective, dynamic, socially constructed, and there are multiple realities. For the realism paradigm, the reality is perceived to be objective, and that it exists independent of the human thoughts, knowledge or existence but this reality is interpreted through social conditioning (Creswell, 2014). The most used philosophical paradigms in the information systems field are the positivist and interpretivist paradigms. A positivist believes that there is an absolute truth and that is the only truth. In this philosophy, the role of the researcher is to find the true answer and describe it.

This research followed the interpretive philosophical paradigm with a constructivist epistemology and the ontology that reality is socially constructed as indicated with a tick mark in Table 3.1.

Table 3.1: The research philosophies

Philosophical paradigm	Epistemology	Ontology: Reality is	
Positivism	Empiricism	Objective and independent of the social actors.	
Interpretivism	Constructionism	Subjective and socially constructed.	✓
Realism	Critical realism	Objective, and exists independent of human thoughts, knowledge or existence, but through social conditioning.	

Table 3.1 has been used to highlight the research philosophies discussed in this section and emphasise the one that was selected and applied in this research study.

An interpretivist is of the view that reality is too complex to control every variable in it. The role of the interpretivist researcher is to find a coherent way of understanding a situation within its natural setting. In critical theory, a critical researcher assumes that reality is socially constructed by people historically over time.

The interpretivist paradigm is supported by Blaxter, Hughes & Tight (2006), Creswell (2009) and Mackenzie & Knipe (2006) as one that is suitable for a case study research method to develop a theory or observe trends in data as patterns of meaning. According to Wynn and Williams (2012), the interpretivist researcher tends to focus on understanding the subjective meanings within a context with reference to a specific phenomenon. Likewise, in this study, the researcher aimed to understand the existence of ambiguities that occur in InfoSec policy wording and the effect of such ambiguities on policy clarity and subsequent compliance.

The ontology associated with interpretivism suggests there is no single reality and that reality is socially constructed by the experiences of the researcher (Mouton, 2011; Oates, 2006). Similarly, the knowledge in this study was created from the researcher's interpretation of the data collected. In this type of research, the researcher describes what he or she sees in the data and his or her reality is not created objectively per the empiricist epistemology (Oates, 2006; Creswell, 2014).

When cutting into the research onion, after the research philosophy layer, next is the research approach layer which is discussed in the following section.

3.3. Research approach

Research approaches explain the link between theory and reality (Bryman & Bell, 2015). The research onion in Figure 3.1 presents two types of research approaches namely; the deductive and inductive approach as follows:

3.3.1. Deductive Approach

The deductive approach starts with developing a hypothesis, and then focuses on testing this hypothesis in the research process (Silverman, 2013). The deductive approach is used where the research project looks at whether the investigated phenomena prove or disprove the researcher expectations, relative to prior research (Creswell, 2014). The deductive approach has been considered to be more suitable for the positivist philosophy.

When using the deductive approach, the research process includes a formulation and testing of hypotheses as well as statistical testing of results to an accepted level of probability (Silverman, 2013). However, a deductive approach could also be used with the interpretive research philosophy, where prior research would be used to establish a general theory and knowledge base against which the research results would be tested (Creswell, 2014). Therefore, the deductive approach develops from the general to the particular. On the other hand, the inductive approach moves from the specific to the general as further discussed in the next section (Bryman & Bell, 2015).

3.3.2. Inductive Approach

In the inductive approach, the researcher begins with an observation and searches for patterns in the data (Beiske, 2007). The inductive approach does not require a framework to inform the data collection and thus, the focus of the research can be established after the data collection stage (Flick, 2011). This approach can be used to generate new theories; however, the results of the data analysis could end up fitting into an already existing theory (Bryman & Bell, 2015).

The inductive approach is more suited for the interpretive research philosophy. The inductive approach is seen to reduce potential researcher bias in the data collection stage of interpretive research where there is no theory used to inform the research process (Creswell, 2014). However, this approach could also be used effectively with positivist research methodologies by analysing the data first, and thereafter using any significant patterns in the data to inform how the results are generated.

This research followed an inductive, qualitative, exploratory content analysis method. Qualitative content analysis can be used inductively or deductively. Whether it is used deductively or inductively, the content analysis process consists of three main phases, namely: preparation, organisation, and reporting of results (Polit & Beck, 2012; Elo et.al.2015). An inductive content analysis was used for this study.

In the preparation phase, the researcher collects the suitable data and selects the analysis units (Baxter, 2009). The organistion phase involves creating the categories and coding the data (Elo & Kyngäs, 2008). In the preparation phase of the inductive content analysis, the researcher performs open coding and abstraction, where the codes are created from the meaning found in the data (Baxter, 2009; Elo et.al, 2015). This is the same process that was followed for this study.

For a deductive content analysis, the organisation phase involves developing the categorisation matrix, whereby all the data are reviewed and coded based on the codes from the pre-existing categorisation matrix (Polit & Beck, 2012; Riff, Lacy, & Fico, 2014).

In the reporting phase, the results are described using the content of the categories used to represent and describe the phenomenon, either deductively or inductively (Palinkas, Horwitz, Green, Wisdom, Duan & Hoagwood, 2015). For the purpose of this study, inductive reporting was used. The research methodology for this study has been represented by use of a research onion diagram in figure 1. The research onion diagram is based on Saunders, Lewis and Thornhill's diagram (Saunders, Lewis & Thornhill, 2009).

Inductive means that you are researching to create theory. The process moves in the opposite direction to the deductive approach taking its focus from the working title of the researcher not the existing theory. This means the research goes from research question to observation and description to analysis and finally theory. Therefore, if little research exists on a topic then an inductive approach may be the best way to proceed (Saunders, Lewis & Thornhill, 2012).

Deductive means that you start with a statement or question and your research sets out to answer it. The aim would be to conclude with a yes or no response to the question. Questions may be statements or informed speculation about the topic that the researcher believes can be answered. The thought process of deduction moves from theory to the research question, to data collection, findings to a rejection or confirmation of the research question. This should lead to a revision of the theory and often starts the process over again (Saunders, Philip Lewis & Thornhill, 2012).

The archival research strategy centres its data collection on existing data sets or archive documents. This allows for exploratory, explanatory or descriptive analysis.

In order to generate results, there are research methods to be followed. The research methods are discussed in the next section.

3.4. Research methods

A research method is the manner in which the data is collected and analysed. It includes the underlying assumptions to the research design as well as the type conclusions drawn and generalisations made from the data (Myers, 2013).

There are two prominent research methods, namely, the quantitative and qualitative methods. A third method can be derived by using a combination of the two, and is referred to as the mixed methods (Bryman & Allen, 2011; Creswell, 2014). The type of method used, depends on the nature of the research, the research context and purpose (Myers, 2013). The two methods are discussed in the next sub-sections.

3.4.1. The Quantitative method

The quantitative research method uses numerical data with the aid of statistical tools for analysis (Creswell, 2014). The statistical tools used in quantitative methods are also used to test for the validity and reliability of the data analysis. Quantitative methods are often used to test theories or explanations and to prove or disprove hypotheses (Myers, 2013). The quantitative method can be used for the purpose of establishing cause and effect.

This method is most effective when there is a large number of respondents available, and the data can be quantitatively measured using statistical methods and quantitative techniques (Bryman & Allen, 2011). The quantitative research method is informed by the positivist philosophy, whereas the qualitative method is informed by the interpretive research philosophy (Ezzy, 2013). The next section discusses the qualitative method in more detail.

3.4.2. The Qualitative method

The qualitative research method is usually used to examine the meaning of social phenomena, rather than seeking a causal relationship between established variables (Bryman & Allen, 2011; Creswell, 2014). Qualitative research involves studies that use textual data in the form of words or languages and do not use statistical procedures for data analysis (Leary, 2016).

Qualitative methods are useful in obtaining an in-depth understanding of a particular situation (Mouton, 2011). Qualitative methods also help to obtain a detailed understanding of a specific context (Ezzy, 2013). This study used qualitative methods. The reason why this study followed a qualitative approach was to focus on the details of the Higher education, institutional InfoSec policy documents as the context and not a generalisation of a broad range of contexts, such as corporate InfoSec policy documents. The choice of research method, affects the research strategies to be used. The research strategies are discussed in the next section.

3.5. Research Strategy

A research strategy is a how the researcher plans to conduct the research work (Creswell, 2014). The research strategy includes the way in which the research aim and objectives will be addressed and how the research questions will be answered (Ezzy, 2013). There are different research strategies available within information systems research, such as experiments, surveys, case studies, archival studies, ethnography, grounded theory, interviews and systematic literature review (Hofstee, 2006; Leary, 2016; Swanborn, 2010).

This study used the case study research strategy. The case study strategy is about rich data, and having an in-depth look at the phenomenon under study, in its natural setting (Mouton, 2011). The chosen case for this research was a University in South Africa, and unit of analysis was the InfoSec policy document of the chosen university. The selected strategy was seen to be relevant and justified by the notion that it facilitated the answering of the chosen research questions posed in Chapter 1.

A rationale for studying this particular case was that there were possible occurrences of ambiguities within InfoSec policies and any such occurrence could lead to user misinterpretation of the institutional InfoSec policies. The potential misinterpretation of the institutional InfoSec policies could subsequently lead the users to breach or violate the InfoSec policy resulting in non-compliance of the InfoSec policy.

The selected case for analysis was therefore worth a comprehensive investigation, as it could contribute to an improvement in InfoSec policy compliance; thereby securing the institution’s information systems from potential user-related security violations and reducing internal InfoSec threats.

Within the research strategy in use, the researcher still has to select the period in which the research project would be conducted. This aspect is also referred to as the time horizon as discussed in the next section.

3.6. Time horizon

The time horizon is the period of time within which the research takes place, the time between the start and intended completion of the research (Saunders, Lewis & Thornhill, 2012). The research onion presents two types of time horizons, the longitudinal and cross sectional (Saunders, Lewis & Thornhill, 2012).

The longitudinal time horizon refers to performing repetitions of collecting data over a lengthy period of time (Goddard & Melville, 2004). The longitudinal time horizon is often used when one of the key research factors involves reviewing change over time (Mouton, 2011). This time horizon helps in studying development and change over time.

A research project with a cross sectional time horizon refers to a research study where the data is collected at a point in time and not repeated (Bryman, 2012). The cross sectional time horizon is also known as the ‘snapshot’ time collection, where the data collected is likened to taking a snapshot of the phenomenon under study, at that point in time (Flick, 2011). The cross sectional time horizon is used to study a phenomenon at that particular time period. This research project used a cross sectional time horizon to study the InfoSec policy documents at a point in time.

The choice of time horizon is not reliant on the research approach (Saunders, Lewis & Thornhill, 2012). The choice of time horizon does however affect the data collection and the availability of data. The following section presents more detail on the data collection and analysis techniques used in this study.

3.7. Data collection and analysis techniques

Data collection and analysis is dependent on the methodological approach used (Bryman, 2012).

3.7.1. Data sampling

A random sample of InfoSec policy documents was collected online for the initial analysis. This initial analysis was done to derive, test and establish themes or categories to be applied to the chosen research sample of data. The data-collection instrument selected for use in this research was an online document collection of existing higher education InfoSec policy documents.

Thereafter, a purposeful sampling strategy was used to select a sample case of one higher education institution in South Africa as it relates to the objectives of the study. (Gerring, 2004; Fereday & Muir-Cochrane, 2006; Wynn & Williams, 2012). The InfoSec policies of the sampled institution were collected for data analysis. Before the documents could be collected from the institution, permission was sought from the institution to proceed with collection and analysis of the documents.

The sampled institution had ten separate InfoSec-related policy documents. Therefore, the sample size collected was a total of ten InfoSec-related policies. The collected policies were treated as sections of the same policy during the content analysis. The policy names were as follows:

The collected ICT policy documents were named P1 to P10 respectively for the sake of participant anonymity of the institution.
Purposive sampling was used to select these policies for ease of access. All ten ICT policies from the institution were used. These constitute the complete population of the institution's ICT-related policies.

The policies were the following:

- P1: Data Privacy Policy
- P2: ICT Asset Disposal Policy
- P3: ICT Mobile Device Policy
- P4: ICT Policy on Broadband Agreements
- P5: Information Security Policy
- P6: Interception and Monitoring Policy
- P7: Internet and Electronic Communication Policy
- P8: Policy on Sending SMS and Emails to Students
- P9: Telephone and Cellphone Policy
- P10: Data Backup Policy

In general, an institution could have one InfoSec policy with subsections addressing other InfoSec aspects as subsections; alternatively, an institution could have a separate sub-policy for each InfoSec subsection. The scope of this research was limited to user InfoSec policies and did not extend to the inclusion of system InfoSec policies. The next section discusses how the collected data was analysed.

3.7.2. Data analysis

A case study approach with a thematic content analysis was used. Mackenzie and Knipe (2006) confirm that document analysis could be used with a case study method. The AtlasTi qualitative data analysis software program was used to perform the content analysis and coding process (AtlasTi, 2016). A process of emergent thematic content analysis was employed to interpret the raw data (cf. Fereday & Muir-Cochrane, 2006; Stemler, 2001). Content analysis is defined as a systematic, replicable technique for compressing many words of text into fewer content categories based on explicit rules of coding (Fereday & Muir-Cochrane, 2006).

Content analysis enables researchers to analyse large volumes of data with relative ease in a systematic fashion (Stemler, 2001; Riff, Lacy, & Fico, 2014). The data-coding approaches available for document analysis are a priori coding and emergent coding schemes. With a priori coding, the categories are established prior to the analysis; whereas with emergent coding, the categories are established based on some initial examination of the data (Boyatzis, 1998). The emergent coding scheme was applied in this study.

The researcher decided on the categories as guided by the literature as well as patterns in the data, and the coding was applied to the data. InfoSec policy statements were reviewed for ambiguity, and the ambiguous statements were grouped into different categories. Data with similar characteristics were grouped into the same category. Revisions were made as necessary, and the categories were revised to an extent of maximising mutual exclusivity and exhaustiveness (Hofstee, 2006; Riff, Lacy, & Fico, 2014).

Method rigor was demonstrated through the process of thematic analysis in which the collected data were examined and searched for themes that emerged and were noted to be indicating the presence of ambiguity, the phenomenon under study (Fereday & Muir-Cochrane, 2006). The content analysis process involved careful reading and re-reading of the data to identify similar features or any recurring patterns within the data. The emerging themes became the categories for analysis (Boyatzis, 1998).

The policy documents were reviewed and analysed to identify the occurrences of ambiguous statements. The types of ambiguities identified within these policy documents were grouped by their common elements and categorised into themes (Oates, 2006). The occurrences of ambiguous statements in the policy were presented using a table as a visual aid to reflect the ambiguous aspect of the policy statements and their related category and depict any trends in the data (Oates, 2006; Riff, Lacy, & Fico, 2014). The researcher used the data analysis results to develop a framework for reducing the occurring types of ambiguities, so as to inform practice.

Irrespective of the chosen research approach, there are two types of data that can be collected, secondary data and primary data. Secondary data are data that has been derived from prior research in the work of others (Newman, 1998).

Primary data are data collected directly from the data sources (Bryman, 2012). Direct sources include survey or interview respondents, and existing documents (Flick, 2011). This study used primary data in the form of existing InfoSec policy documents. When the aspects of the research onion layeys have been applied according to the research objectives, the process followed in executing the steps is the research methodology. The research methodology for this research is discussed in the next section.

3.8. Research methodology

This section presents the research methodology, which is the research process that was followed for this study. A research methodology, also referred to as a research design is defined as a plan and description of how a research project was carried out (Mouton, 2011). The research design pays closer attention to the research artefact or end product.

The methodology departs from the research problem and the type of data required for addressing the research problem. And focuses on the research tools used and procedures followed (Ezzy, 2013). The chosen methodology for this study applied qualitative tools and techniques, as they were most suitable in addressing the research objectives and answering the research questions posed in Chapter 1.

The methodology includes the complete research process followed, starting with the identification and selection of suitable data sources, data collection tools, methods of analysis and subsequent interpretation of the results (Yin, 2009).

Research methodology can be categorised as empirical or non-empirical. Empirical studies include quantifying and observing reality to subsequently verify knowledge through direct experience. Non-empirical studies, also referred to as theoretical studies, are concerned with exploring as well as developing theories that account for and justify the research data (Creswell, 2009).

Empirical studies could use textual data, numeric data or a combination of the two. When textual data such as words are used for an empirical study, the study would be categorised as a qualitative study. Alternatively, when numeric data are used, the study would be categorised as a quantitative study. A research design could also combine the qualitative and quantitative methods to achieve more reliable results than when using each method on its own (Ezzy, 2013).

Mouton (2011) asserts that in terms of the research questions posed for a study, there is a differentiation between empirical and non-empirical questions. Empirical questions address real-life questions and non-empirical questions address theoretical or conceptual model questions. Empirical questions are said to involve non-scientific knowledge, which refers to lay, everyday knowledge; while non-empirical questions would involve generating valid, reliable descriptions, models and theories of the world in search of scientific truth (Mouton, 2011).

For the purpose of this study, the following non-empirical questions were posed in section 1.5 of Chapter 1 as follows:

- *SRQ1*: What does literature on InfoSec policies say about InfoSec policy issues?
- *SRQ 2*: What are the main problems with InfoSec policy compliance?
- *SRQ 3*: What are the main problems relating to ambiguity within InfoSec policies?
- *SRQ 4*: *How can InfoSec policy ambiguities be reduced to improve policy compliance and clarity?*

Non-empirical methods were followed in order to answer these research sub-questions. A literature review was conducted, which included a document analysis in order to address the first three research sub-questions. A model-building approach was used to answer the fourth research sub-question. These methods used textual data and subsequently this study is categorised as a qualitative study. This study was therefore a non-empirical, qualitative study.

3.8.1. The research process

The research process was executed in the steps depicted in the conceptual framework in Figure 3.2. To address the first three research sub-questions, the research started with a systematic literature review. The literature review is presented in Chapter 4 as an analysis with its related results, with aspects of it in Chapter 2 as part of the foundational literature for the study. In addition, a document analysis was conducted on the contents of InfoSec policy documents sampled from a higher education institution. The results of the document analysis (content analysis) are presented in Chapter 4 as research findings.

A model-building approach was used to build a framework and address research sub-question 4. The model building is presented in Chapter 5 in the form of suggested solutions to reduce the occurrence of ambiguity in InfoSec policies. The model-building aspect of the study depended on the results of the document analysis from Chapter 4. Furthermore, application scenarios were provided to strengthen the validity and reliability of the research. The application scenarios were used to test the recommended theoretical solutions. These research process steps are diagrammatically represented in Figure 3.2.

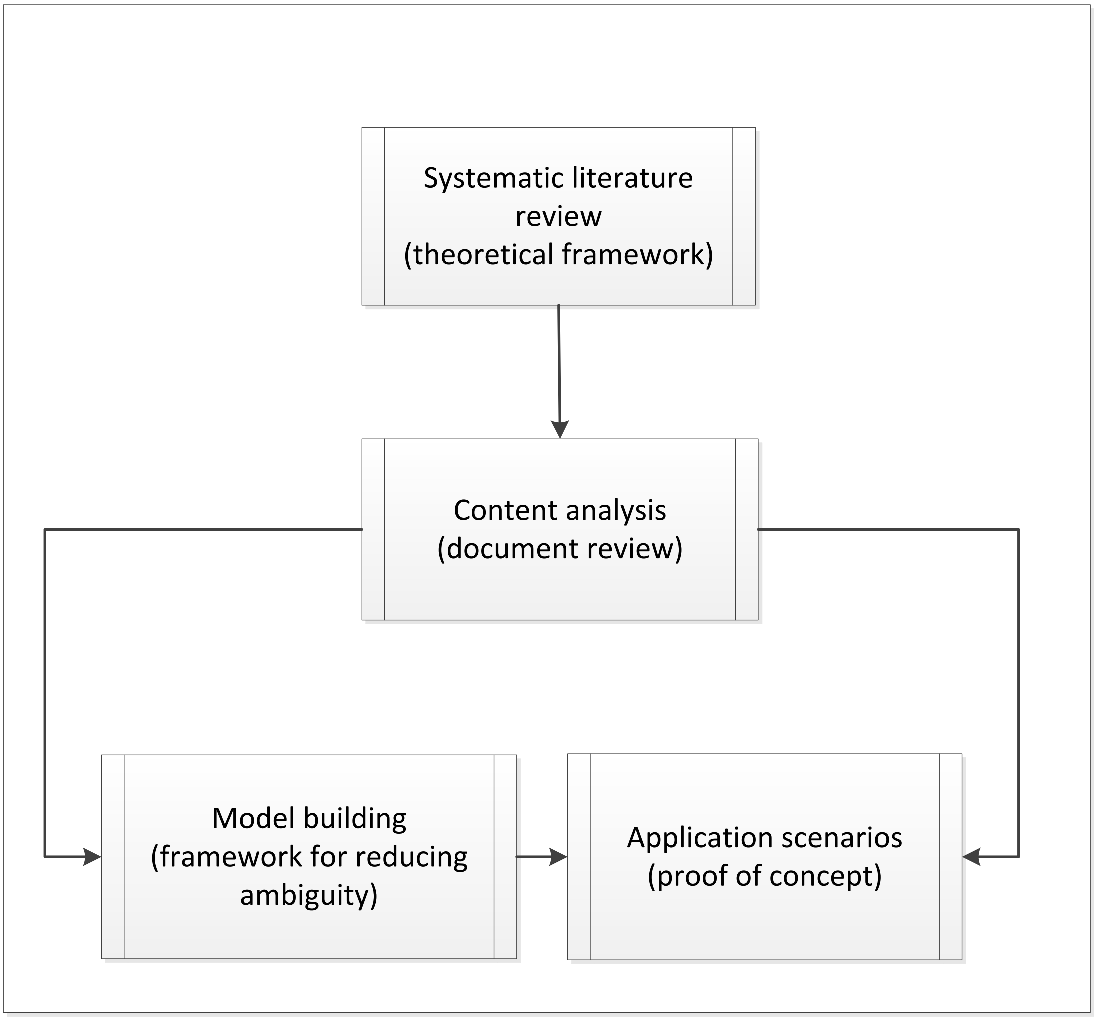


Figure 3.2: The research process conceptual framework (Synthesised by researcher)

The following sections discuss the research process of Figure 3.2, starting with the systematic literature review in section 3.8.2. Followed by the content analysis in section 3.8.3, the model building in section 3.8.4 and finally, the application scenarios in section 3.8.5.

3.8.2. Systematic literature review

A literature review is defined as a study that presents an overview of scholarship in a specific field through analysis of trends and the published work of others (Hofstee, 2006; Mouton, 2011). A literature review relies on secondary literature to highlight trends in the research area at hand and it also helps in identifying empirical and theoretical weaknesses in the published works (Yin, 2009). These weaknesses are often referred to as the research gap (Leary, 2016).

A literature review also constitutes a non-empirical study with the unit of analysis being data from the collected literature in the area of study (Mouton, 2011). In order to contextualise and understand how to address the research questions posed for this research project, it was necessary to determine what problems InfoSec policies presented by way of a literature review.

A systematic literature search was performed to gather background literature on the work performed in the area of InfoSec policy compliance and to identify a research gap that this research project could address (Stemler, 2001; Yin, 2009). The choice of literature sources was based on the research objectives; questions to be addressed and the available time to conduct the study (Leary, 2016). Literature reviews use inductive reasoning to understand a said domain of scholarship from the chosen sample of reviewed text (Mouton, 2011).

A systematic literature search process was adopted to ensure validity and reliability. In this review, reliability is based on selected databases, publications, the covered period and keywords used for the literature search, which are documented for replication of the literature search process. Academic articles in the field of InfoSec in policy management and the compliance contexts were included.

The rating of the journal, the research methodology and geographic region of the research were disregarded and not used as inclusion or exclusion categories. This was to ensure there is a sizeable collection of literature to review. However, non-academic articles (white papers and industry magazine articles) were excluded due to lack of methodological rigour. A language restriction was imposed, where only articles in English were included.

In total, 382 articles were downloaded for further processing. The downloaded articles were screened to exclude those focused on testing user InfoSec awareness and 167 articles remained. To verify the relevance of the collected articles to the context under study, abstracts were read, and in some instances, other parts of articles were reviewed to identify the most relevant and applicable articles. As a result, 67 articles were deemed useful for this study.

For reliability of the literature review, a list of keywords was developed prior to the literature search to focus on relevant studies (cf. Hofstee, 2006). The list of search keywords is noted in Table 3.2 and the searched databases are listed in Table 3.3. The results of the literature review are presented in Chapter 4.

Table 3.2: List of keywords and phrases used for literature search

#	Searched keywords
1	Information security policy issues
2	IT security policy
3	IT governance policy
4	Information security management policy
5	Security policy problems

6	Security policy compliance
7	Information security policy management framework
8	Information security framework

Table 3.3: List of databases and search engine used for literature search

No.	Name of database	No.	Name of database
1	Academic Search Complete	2	Brill
3	Business Source Complete	4	Cambridge Journals Online
5	Computers & Applied Sciences Complete	6	EBSCOhost EJS
7	Emerald Management e-Journals	8	Sage Journals Online
9	Science Direct	10	Google Scholar (search engine)

Soomro, Shah, & Ahmed (2016) conducted a similar literature study, as they investigated the necessity for what they refer to as a more holistic approach to InfoSec management. They found that technological InfoSec solutions are rapidly developed; however, InfoSec issues remain a huge challenge for organisations. They report that the challenges remain because these technological solutions depend on InfoSec policy and organisational strategies. Soomro, Shah, & Ahmed (2016) further concluded that security policies and organisational strategies should be explored from a managerial point of view.

Grant, Edgar, Sukumar & Meyer, (2014) focused on literature in the decade between 2004 and 2014, whereas in the current literature review, the period exclusion category was removed in order to capture even the earliest views recorded about the meaning of and need for InfoSec policies. Therefore, the inclusion category for the collected literature was all periods to date, as the time when this study was conducted in 2016.

Relative to the study by Soomro, Shah, & Ahmed (2016), which focused on recent developments of the past decade in the area of InfoSec management, this study focused particularly on the human aspects of InfoSec management as they relate to InfoSec policy use and awareness since inception of the information age.

3.8.3. Content analysis

In this research, an inductive process of emergent thematic analysis was employed in order to interpret the raw data (cf. Downe-Wamboldt, 1992; Fereday & Muir-Cochrane, 2006). A sample of higher education InfoSec policy documents collected online was inductively reviewed to derive themes from the data.

These themes were later applied to categorise the ambiguities in the purposeful sample (refer to Section 4.3).

Content analysis is defined as a systematic, replicable technique for compressing many words of text into fewer content categories based on explicit rules of coding (Stemler, 2001). Content analysis enables researchers to go through large volumes of data with relative ease in a systematic fashion (GAO, 1996). The data-coding approaches available for document review are a priori coding and emergent coding schemes (Downe-Wamboldt, 1992; Fereday & Muir-Cochrane, 2006). With a priori coding, the categories are established prior to the analysis, whereas with emergent coding, the categories are established based on some initial examination of the data (Stemler, 2001).

3.8.3.1. Emergent data coding

For this study, a template was developed based on the research questions and theoretical concepts (cf. Fereday & Muir-Cochrane, 2006). In order to understand how InfoSec policies are documented, an emergent coding approach to document reviews was conducted on a sample of InfoSec policy documents. Emergent coding is a deductive way of coding the data based on themes developed while analysing the data; the codes emerge from the data (Stemler, 2001). InfoSec policy documents as well as best practice documents were collected online and used for the document analysis. The emergent coding process was followed to develop themes from the statements and phrases in the policy documents that were reviewed.

For this study, codes were written based on that of Boyatzis (1998) and identified by the following characteristics:

- The code label or name
- The definition of what the theme concerns
- A description of how to know when the theme occurs.

During data analysis, the process of emergent thematic content analysis was used in order to analyse and interpret the data. The emergent data-coding scheme was applied to the data. The ambiguity types were used as themes for coding the data. The resulting thematic codes are documented in Table 3.4.

Table 3.4: Ambiguity themes

Code	Thematic codes		
	Code name	Definition	Description
SeLA	Structural/Semantic/Lexical ambiguity	Language-related Grammatically unclear and semantically ambiguous statements	The statement is broad and could be abused to refer to unintended outliers.
VID	Vague/Implicit description	Implicit statement The content is alluded to but not explicitly mentioned Assume user background knowledge	The statement is vague and lacks clarity of detail.
ONP	Omission/Null pointer	Content referred to is not available or accessible	The statement refers to an item that is not at the said location.
DN	Double negative	Statement uses two double negatives to infer a positive meaning, which could potentially be confusing User is told what not to do User first has to interpret the statement in terms of its positive version to find out what to do	The statement is phrased using antonyms of the intended meaning with a negative connotation.
CON	Contextual	Contextual misplacement Statement is placed in the wrong section of the document	The statement is documented with unrelated statements in the document.

Each identified ambiguous phrase was categorised into the theme that best describes the phrase’s characteristics that make it ambiguous. From the six types of ambiguities from literature in chapter 2, the following themes were derived for this study: All the grammar-related ambiguity types were grouped into the SeLA (structural/semantic/lexical ambiguity) theme; the implicit statements were grouped into the VID (vague/implicit description) theme; all the references made to documents that were not accessible were categorised into the ONP (omission/null pointer) theme; and the occurrence of double negatives was categorised into the DN (double negative) theme. Where a statement was documented in an unrelated policy section, the occurrences were categorised in the CON (contextual) theme for contextual misplacement as noted in Table 3.4.

Once the themes were identified, the data were re-read and categorised into their most suitable respective themes. The identified ambiguous statements were grouped into different categories. The category names were derived from known types of ambiguities as noted from prior research per the literature review step of the research process.

The phrases that possessed the properties of any of the listed themes were documented in a table and further reviewed for overlaps or further clarity. Some phrases were removed from the table after consultation and discussion with the research supervisors, i.e. those phrases were deemed subjective. These phrases were initially thought to have been unclear, but were deemed subjective given reasonable doubt. A secondary review of the documents P1-P10 was performed using AtlasTi to identify ambiguous words per the established themes from the initial analysis.

The results of the coding process reflecting the subjective phrases from the reviewed policies are documented in Chapter 4. The following section discusses the model-building aspect of the study.

3.8.4. Model building

According to Mouton (2011), model-building studies aim to explain the phenomenon under study by way of developing new theories and models. A model is a process or system outline used to clearly and concisely represent a certain phenomenon (Mouton, 2011; Leary, 2016). A model is an abstract representation of parts of the real world and represents the main aspects of a system or process, often omitting the nonessentials (Aveson & Fitzgerald, 2006). A model represents a system in the form of its components, roles and interfaces within the system (Leary, 2016). The model generally provides a simplified, comprehensible, yet exact representation of the world, which makes it useful for problem solving in research (Leary, 2016).

Model-building studies are also said to be non-empirical (Leary, 2016). These studies use secondary data from an existing body of knowledge, such as literature. Model building can be performed with deductive or inductive reasoning (Mouton, 2011). Deductive reasoning is more formal due to its use of a set of axioms formulated and used to deduce additional theoretical propositions. Alternatively, inductive reasoning is generally used in statistical model building, where a model is used to explain particular empirical data (Yin, 2009). For non-empirical qualitative research, inductive reasoning is often used. The same was used for this study to develop a framework for reducing ambiguity as it occurs within InfoSec policy documents. The model building aided the researcher in addressing the fourth research sub-question.

The results of the model-building aspect of the study are presented in Chapter 5 of this dissertation in the form of proposed solutions to the ambiguity problem. The next section explains the application of the model framework as a proof of concept.

3.8.5. Application scenarios

Application scenarios were used in the study to provide an in-depth description of a limited number of case scenarios. Application scenarios allow specific cases to be focused on and studied in more detail without having implemented the model in real life (Aveson & Fitzgerald, 2006). Application scenarios were used in this study because the proposed framework had not been implemented at the time of this study. Application scenarios are empirical in nature and are suitable to be used in qualitative or quantitative studies (Leary, 2016).

There are two techniques that are often used for the selection of cases to use for application scenarios, namely literal replication and theoretical replication. For literal replication, the cases are chosen such that they use extreme cases to test the theory. In the theoretical replication instance, cases are selected such that the theory applies in some cases and not in others (Leary, 2016).

The disadvantage of application scenarios, just like that of cases studies, is that it lacks the generalisation of results and non-standardisation of measurements (Mouton, 2011). To obtain more general results, multiple case scenarios are used.

The potential bias of the researcher, especially in case selection, may lead to results of limited value (Mouton, 2011). The advantage of application scenarios is that they are able to combine qualitative and quantitative data in one case (Leary, 2016). The purpose of using application scenarios in this study was to apply the suggested solutions to the problem areas that were identified in the content analysis of the study and to demonstrate the utility of the suggested solutions as a proof of concept. The proof of concept was used in this study in order to strengthen the validity of the research results. The application scenarios were applied in the form of example applications of the different recommended solutions per problem category, as contained in Chapter 5.

The next section discusses the steps followed to ensure that the research was performed ethically.

3.9. Ethical considerations

Ethical clearance was granted for the study by the research committee in the School of Computing at Unisa. This ethical clearance requires the researcher to maintain the confidentiality and anonymity of any parties who participated in the study, so that they are not easily recognisable as referred to in the study. The ethical clearance certificate is attached in Appendix A.

3.10.Chapter summary

This chapter provided the philosophical paradigm perspective of the research as well as the research design and methodology pertinent to the study. The chapter presented the processes and procedures followed in the study. These processes were informed by literature in selecting the most suitable research methods and tools for the chosen type of research. The data-collection tools and the data-analysis were also discussed.

The next chapter discusses the research results and findings after the research methods were applied in the research process.

Chapter 4
Data Analysis and Findings

4.1. Introduction

The previous chapter outlined the research process steps and related research methods that were applied in this study.

The research aim for this study was to conceptualise a framework for addressing university InfoSec policy ambiguity, to aid InfoSec policy compliance.

The research objectives for this study as noted in section 1.5.2 were:

- *RO1*: Explore the literature on InfoSec policies;
- *RO2*: Identify the main problems facing InfoSec policy compliance;
- *RO3*: Identify the main problems relating to ambiguity within InfoSec policies;
- *RO4*: *Define how InfoSec policy ambiguity can be reduced to improve compliance and clarity*

The first and second research objectives, RO1 and RO2 were addressed in the form of a systematic literature review in section 4.2. The third research objective, RO3 was addressed by means of a content analysis in section 4.3. The fourth research objective was addressed by means of the proposed solutions and framework in Chapter 5.

The next section reflects the research results and findings obtained after applying the research methods to address the research objectives. The result discussions include the outcome of the systematic literature review and the content analysis as discussed in the research process and methodology of Chapter 3. The next section initiates the results discussion by presenting the results of the systematic literature review.

4.2. Systematic literature review results

In order to contextualise and understand this research, it was necessary to comprehend the challenges facing InfoSec policies. Therefore, a systematic literature search was performed. A rigorous literature search process was adopted to ensure validity and reliability. In this review, reliability is based on the selected databases, publications, the covered period and keywords and key phrases used for the literature search, which are documented for replication of the process.

The systematic literature review included academic articles in the field of InfoSec policy management as well as the policy compliance. The list of databases is provided in section 3.9.2 where the systematic literature review research process was presented in detail. Subsequently, this section presents the results of the systematic literature review. The following concepts emerged in the literature as the most occurring barriers to InfoSec policy compliance.

4.2.1. Barriers to information security policy compliance

During the analysis of the identified literature, which involved determining what other scholars have reported as the barriers to InfoSec policy compliance, the following were reported to be the main factors affecting compliance:

- Lack of management support for information security presented in Table 4.1;
- Organisational culture presented in Table 4.2;
- Information security policy awareness and training in Table 4.3;

- The importance of the human aspect for information security management in Table 4.4; and
- Information security policy clarity in Table 4.5.

The listed factors are discussed sequentially in the next sections.

4.2.1.1. Lack of management support for information security

In a study conducted by Humaidi & Balakrishnan (2015) among health professionals, their results indicated that management support, particularly leadership styles supportive of InfoSec initiatives, proved to influence InfoSec policy compliance behaviour, depending on whether the leadership was actively supportive of InfoSec initiatives. The InfoSec initiatives were more successful when management actively supported them. Further literature that presented similar views about management support for InfoSec is presented in Table 4.1.

Table 4.1: Relevant literature on lack of management support for information security

Lack of management support for information security	
Author(s) & year	**Findings**
Chang & Ho (2006)	A firm should have a comprehensive management structure and practices for InfoSec. There should be formal structures of InfoSec management within an organisation.
Knapp, Morris, Marshall & Byrd, (2009)	Top management support is the most critical issue of an InfoSec programme and its success.
Ezingeard & Bowen-Schrire (2007)	Top management interest and participation are vital for continued improvements within InfoSec systems.

Ma, Schmidt & Pearson (2009)	Management support is possibly the most important component of effective InfoSec management.
Hu, Dinev, Hart, & Cooke (2012)	Top management participation in InfoSec management has a significant influence on employees’ attitude and behaviour in terms of their compliance with InfoSec policies.
Whitman & Mattord (2012)	Safe and secure operation of information assets is a senior management responsibility.
Kwon et al. (2012)	Top management involvement in policy formulation has a positive impact on InfoSec effectiveness.
Phillips (2013)	Management practices have a significant role in IT system effectiveness.

Table 4.1 presented the most significant literature indicating that one of the problems with InfoSec policy compliance is the lack of management support. Therefore, it becomes clear that active and supportive management attitudes towards InfoSec initiatives within organisations, including higher education institutions could improve the InfoSec policy compliance. The participation of top management participation in InfoSec initiatives has been noted to have a significant impact on employees’ attitudes towards policy compliance (Hu, Dinev, Hart and Cooke, 2012).

Organisational culture was the next significant aspect affecting InfoSec policy compliance, according to the systematic literature review. The organisational culture as it relates to InfoSec policy compliance is discussed in the next section.

4.2.1.2. Organisational culture

Organisational culture can affect user compliance with the InfoSec policy, based on what is deemed as acceptable behaviour among fellow employees. Siponen & Vance (2010) refer to this phenomenon as an ‘appeal to higher loyalties’. Table 4.2 presents more literature related to organisational culture and how it affects compliance.

Table 4.2: Relevant literature on organisational culture

Organisational culture	
Author(s) & year	**Findings**
Da Veiga & Eloff, (2010)	A security conscious organisational culture can help improve InfoSec policy compliance.
Thomson, Von Solms & Louw, (2006)	Organisations should be more receptive of InfoSec initiatives.
Siponen & Vance (2010)	Policy users will comply with the policy if compliance is perceived positively by their colleagues and therefore Organisational culture affects InfoSec policy compliance.
Van Niekerk, , R. Von Solms (2010)	Cultivating an organisational sub-culture of InfoSec can help address the problem of users violating the policy, whether intentionally or unintentionally and thereby addressing the “insider human threat” to InfoSec.
Crossler, Johnston., Lowry, Hu, Warkentin & Baskerville (2013)	It is important organisational management teams to encourage a culture of InfoSec awareness and compliance. A culture of compliance could reduce policy violations.

A security-aware culture would encourage InfoSec policy compliance (Da Veiga & Eloff, 2010). Organisations should cultivate an InfoSec-receptive culture (Thomson, Von Solms & Louw, 2006).

The next barrier that was reported to be affecting user compliance is the InfoSec policy awareness and training. This concept is discussed in the following section.

4.2.1.3.Information security policy awareness and training

There is great importance placed on user InfoSec awareness and training for better InfoSec policy compliance (Danchev, 2003). Insufficient InfoSec policy awareness and training have been attributed to user non-compliance with the InfoSec policy (Siponen, Mahmood & Pahnila, 2014). Therefore, educating the users could increase policy compliance. Further literature discussing InfoSec policy awareness and training in relation to policy compliance has been presented in Table 4.3.

Table 4.3: Relevant literature on information security policy awareness and training

Information security policy awareness and training	
Author(s) & year	**Findings**
Gerber, Von Solms & Overbeek (2001)	Management should develop the InfoSec requirements to focus more on information and not only on infrastructure. They illustrate that InfoSec requirements could be used to determine the required level of InfoSec, as opposed to using a risk analysis.
Danchev (2003)	Security can be improved by properly educating staff on their role in protecting organisational resources. This education and training should be varied and evolving to keep the staff continuously interested and well informed. The education initiatives could include developing a security awareness programme, a security newsletter, security articles, explaining new threats and technology trends.
Whitman (2004)	InfoSec needs higher levels of awareness, education and policy.
D'Arcy, Herath, & Shoss (2014)	IT management should develop effective security policies, identify critical assets and encourage communication between IT and risk managers.

Chang & Lin (2007)	Effective security policy and practice are vital for InfoSec, as technical measures alone are not sufficient for this purpose.
Hagen, Albrechtsen & Hovden (2008)	InfoSec awareness creation is more effective than other measures.
Siponen, Mahmood & Pahnila (2009)	The visibility of the InfoSec policy has a positive impact on employees' behaviour towards policy compliance.
Ma et al. (2009)	InfoSec training is possibly the most important measure for its effectiveness, as it increases awareness and understanding.
Doherty, Anastasakis & Fulford (2009)	Security breaches can be reduced by protecting a firm's information through an effective InfoSec policy.
Puhakainen & Siponen (2010)	InfoSec policy compliance training has a positive effect on employees' behaviour in terms of compliance.
Albrechtsen & Hovden (2010)	Employee participation and knowledge creation incorporate positive changes towards InfoSec awareness and behaviour.
Johnston & Warkentin (2010)	Policies and user awareness training are necessary controls to support technical security controls.
Rubenstein & Francis (2008) in Soomro, Shah, & Ahmed, (2016)	A major internal threat to InfoSec is access policy violation with malicious intentions.
Singh, Picot, Kranz, Gupta & Ojha (2013)	A comprehensive policy and effective management process for its implementation are necessary for InfoSec management.
Dagada & Eloff (2013)	They found that some users perceive the InfoSec policy to be a nuisance, as it restricts user freedom to particular aspects in the information systems.
Siponen et al. (2014)	InfoSec awareness has a significant impact on employees' compliance with InfoSec policies.

Parsons et al. (2014)	Awareness training and education have a positive impact on employee attitude and behaviour towards InfoSec policy.

Table 4.3 presented the most significant literature on InfoSec policy awareness and training and how it affects policy compliance. Essentially, awareness and training have been reported to increase compliance, by use of quantitative studies (Albrechtsen & Hovden 2010; Parsons et al., 2014).

The next concept affecting InfoSec policy compliance was reported to be the human aspects of information security, generally referred to as human vulnerabilities and human error. This concept is discussed in the next section.

4.2.1.4.Human aspects of information security management

It is often said that the weakness of any security system are the human users (Parsons et al., 2014). This people-based weakness has also been referred to as human-based InfoSec vulnerabilities (Furnel & Peppard, 2007; Williams, 2008 ; Parsons et al., 2014).

A 2010 study conducted in Malaysia reported that human error was one of the major internal threats towards implementation of the Health Information System (Narayana, Ahmad & Ismail, 2010). Human error caused InfoSec incidents because employees in the organisation lacked recognition of potential threat vulnerabilities, had undeveloped understanding of InfoSec and lacked knowledge of InfoSec (Humaidi & Balakrishnan, 2015). More literature on this topic was recorded in table 4.4.

Table 4.4: Relevant literature on the importance of the human aspect for information security management

The importance of the human aspect for information security management	
Author(s) & year	**Findings**
D'Arcy, Herath, & Shoss (2014)	InfoSec managers should consider human aspects of InfoSec.
Trček, Trobec, Pavešić & Tasič (2007)	The most important factor behind ensuring InfoSec is humans, because in every InfoSec system, there is complex interplay between humans and technology.
Chang, Wang & Shen (2010)	In addition to technical security threats, there are attacks such as social engineering, which targets the human element.
Yeniman et al. (2011)	The most common security vulnerability has been human carelessness; the human factor therefore remains the weakest link in InfoSec.
Rhee, Ryu & Kim (2012)	Effective InfoSec management must consider human aspects along with technological dimensions.
Vance, Lowry & Eggett (2013)	Malicious insiders possessing a higher level of knowledge, resources and data access are a big threat to InfoSec as compared to outsiders.
Jaeger (2013)	The major causes of data breaches are employees' errors, rather than hackers.
Dagada & Eloff (2013)	Technical security controls alone are not effective protection mechanisms. There is a need for policies, user awareness and education as administrative security defences to target the human element, which is prone to attacks.

From table 4.4, it is clear that the human element has accounted for InfoSec policy violations and is therefore a significant factor to address in order to improve policy compliance. The insider threat is even more dangerous than external threats, as an insider may easily misuse the skills and knowledge gained through legitimate work duties for illegitimate gain (Willison & Siponen, 2009). The countermeasures used for human-based vulnerabilities in business organisations is the user InfoSec awareness programme as well as the user induction programme.

The last concept noted to be of significance from the literature regarding policy compliance was the InfoSec policy itself, and its clarity as discussed in the next section.

4.2.1.5.Information security policy clarity (the policy itself)

Table 4.5: Relevant literature on information security policy clarity (the policy itself)

Information security policy clarity	
Author(s) & year	**Findings**
Kolkowska & Dhillon, (2013)	InfoSec policy description was inconsistent due to the conflict in functional rules and where several security objectives might have been contradicting one another.
Gerber et al. (2001)	Once the InfoSec requirements have been determined and documented, the adequate security controls are then implemented. One of the most common security controls is the InfoSec policy document. More attention should be paid to securing information assets and not only infrastructure.
Höne & Eloff (2002)	These policies also define the rights and responsibilities of information resource users by helping the users understand what is deemed acceptable and responsible behaviour in handling organisational data and information resources to ensure the safe

	and secure handling of information in performing their organisational duties and responsibility.
Bandara, Lupu & Russo (2003)	They discuss a method for transforming policy and system behaviour specifications into a formal notation that is based on event calculus. They argue against formal logic based systems. Logic-based languages have proved attractive for the specification of a security policy, as they have a well-understood formalism. However, they can be difficult to use and are not always directly translatable into efficient implementation.
Danchev (2003)	The author defines a security policy as a plan outlining a company's critical assets and how they can and must be protected. An InfoSec policy is necessary because it serves as the first measure in reducing unacceptable use of the ICT resources in an organisation. The policy should be "precise yet enforceable". Some elements of a good and well-developed security policy: • Addresses the handling of sensitive information • Details how the personal user ID and password(s) should be properly maintained • States how employees should respond to a potential security incident or suspected security breach or intrusion • Details how to securely use ICT resources, including computers and internet connections • Indicates how to use the organisation's corporate e-mail system.
Rees et al. (2003)	They point out the problem of keeping InfoSec policies consistent.
Von Solms & Von Solms (2004)	The policy should act as the point of departure for employees with respect to all InfoSec issues, and in so doing, it becomes the 'heart and basis' of successful security management.

D'Arcy, Herath, & Shoss (2014)	InfoSec policies have a significant impact on the security of information systems and successful business operations.
Sohr, Drouineaud & Ahn (2005)	They focus on security policies for access control in clinical information systems. They report that these policies are highly dynamic because of their area of application. They define formal specifications of dynamic security policies for clinical information systems. They chose first-order linear temporal logic (LTL) as their formalism of choice and one of their reasons is that it has been intensively studied in the literature. They use first-order LTL to specify role-based access control security policies.
Information Security Policy: A development guide for large and small companies (2006)	The lack of InfoSec policy clarity is noted as a policy-development problem.
Gelbstein (2006)	The organisation has to ensure that the InfoSec policy is available to its intended users, easy to use, updated and kept current.
Saleh et al. (2007)	Employees should have little excuse for not being able to apply defined security practices in accordance with the established policy.
Boehmer (2008)	The ISO/IEC27001 document provides the mandatory requirements for an information security management system. It mandates for the InfoSec policy to govern the day-to-day operations of ICT. It uses ISO/IEC27002 to indicate suitable controls in a security management system. The ISO/IEC27002 is an InfoSec standard published by the International Organization for Standardization.
Parkin, Van Moorsel & Coles (2009)	They developed an InfoSec ontology to better understand the human-behavioural factors within the InfoSec space. They argue that their model can be used to represent the knowledge of

	insider threats and provide details on limiting malicious insider activity. The authors found that it was possible for organisations to consolidate consideration for human factors with compliance with security standards.
Doherty, Anastasakis & Fulford (2009)	The most important role of the InfoSec policy is to make plain the rights and responsibilities of users such that these are made clear and understood by the users. This is to ensure that there is a uniform and consistent institutional view of InfoSec, thereby further emphasising the need to make InfoSec policies explicit, leading to the need to formalise them.
Knapp, Morris, Marshall & Byrd (2009)	Organisations are more dependent on the reliability of their information systems in order to ensure the credibility of their information and decisions. Therefore, there is a need to define the rules that govern InfoSec measures; these rules are contained in InfoSec policies.
Andress (2014)	The authors highlight an important aspect of InfoSec policies, namely that they should be kept current by means of periodic reviews and updates to ensure that they are relevant and applied by their intended users.
Whitman & Mattord (2012)	InfoSec focuses on preserving the critical characteristics of information, such as availability, accuracy, authenticity, confidentiality and integrity. They describe the notion of a good InfoSec policy in that it should encapsulate the responsibilities of individuals, denote what is authorised and unauthorised system use and enable individuals to report suspected or identified threats (whistle blowing); it should define punishment means for policy violations and ways to update the policy to keep up with the constantly changing IT environment.

InfoSec policy clarity as a policy compliance barrier could have a ripple effect on all the other barriers, regardless of how well they have been addressed. Therefore, there should be more focus on increasing policy clarity and reducing ambiguity.

4.2.2. Systematic literature review conclusion

The barriers to InfoSec policy clarity can be addressed as noted in table 4.6:

Table 4.6: Possible solutions to InfoSec policy compliance barriers

Compliance barrier	Possible solution
The lack of management support	Increase active participation in and support of InfoSec initiatives.
Organisational culture	Increase InfoSec policy awareness training.
Lack of InfoSec policy awareness and training	Initiate awareness and training initiatives.
Human aspects of InfoSec policy management	Increase InfoSec policy awareness training.
InfoSec policy clarity	Clarify policy statements.

Table 4.6 presented the possible solutions to the compliance barriers. However, with regards to the policy clarity, irrespective of how much top-management commitment or participation is provided to InfoSec management, an unclear policy could just as well lead the same top management to non-compliance by misinterpretation.

The same holds for changing the organisational culture and increasing InfoSec policy awareness and training. The presence of ambiguity in the InfoSec policy document could render these efforts futile. Therefore, it was deemed essential to investigate the problem of ambiguity in order to gain a better understanding and subsequently address the problem.

The next section presents the results of the content analysis process.

4.3. Content analysis results

For the purpose of the content analysis, an online search was conducted for InfoSec policies of higher education institutions, globally. Two institutions were randomly sampled from the available population and their InfoSec policies were used as the data sample. Each of the sampled institutions had a single policy with multiple sections, as opposed to each section of the InfoSec policy contained in a separate document.

The reviewed InfoSec policies included a random sample of the online InfoSec policy documents from higher education institutions collected online, named OP1-OP2 for the confidentiality and anonymity of the institutions; and a further purposive sample of 10 InfoSec related policies from a single higher education institution, the policies were named P1-P10. The initial content analysis process is detailed in the next section.

4.3.1. Initial Content analysis

The randomly sampled InfoSec policy documents, together with the purposive sample were used for the initial analysis. The initial analysis was done to derive, test and establish themes or categories to be applied as codes on the chosen purposive sample of data. An emergent coding process was followed to develop themes from the statements and phrases in the reviewed policy documents.

The emerging themes were documented as thematic codes as follows:

- Structural/ Semantic/ Lexical Ambiguity (SeLA): Grammatically unclear and semantically ambiguous statements. The statement is broad and could be abused to refer to unintended outliers.
- Vague or Implicit Descriptions (VID): Implicit statement. The content is alluded to but not explicitly mentioned. Assumed user background knowledge. The statement is vague and lacks clarity of detail.
- Omissions and null Pointers (ONP): The content referred to is not available or accessible. The statement refers to an item that is not at the said location.
- Double Negative (DN): The Statement uses a double negative to infer a positive meaning. This could potentially be confusing. The user is told what not to do. They first have to interpret the statement to its positive version to determine what to do. The statement is phrased using negative antonyms of the intended meaning with a negative connotation.
- Contextual (Con): Contextual misplacement. The statement is placed in the wrong section of the document. Such practice may make it hard to locate it. The statement is placed with unrelated statements within the document.

The data were reviewed several times to come up with mutually exclusive themes to categorise the data. Each identified ambiguous phrase was categorised into the theme that best describes the phrase’s characteristics that make it ambiguous. During the iterations of the emergent coding process, some phrases were discarded after consultation and discussion with the research supervisors; i.e. those phrases were initially thought to have been unclear, but were deemed subjective given reasonable doubt. Table 4.7 reflects the subjective phrases from the reviewed policies.

Table 4.7: Subjective policy statements

Document name	Statement	Problem	Researcher comments
OP1	8.11: “Your obligation to protect sensitive information continues after you leave the University”	Ambiguous. Does this only include university-sensitive information or any sensitive information?	Upon analyses, this was noted to be subjective, as it is easy to assume that the statement refers to sensitive information acquired as a user of the institution’s systems.
	13: “If you are performing work in an office that handles information subject to specific security regulations, you will be required to acknowledge that you have read, understand and agree to comply with the terms of this policy annually”	Confusing. The policy should be acknowledged by all who use ICT systems, not only those dealing with information subject to security regulations.	The researcher of the current study seemed to be questioning the institution’s policy scope.
OP2	3.10.3.1. “The IT security manager should be familiar with simple routines for collecting evidence”	This section has only one statement.	This is not a real problem. Vague. What constitutes simple routines and what evidence would they be collecting. Inconsistent.

The remaining phrases after the subjective ones were removed were categorised into their most suitable thematic codes. The occurrences of the themes as observed in the reviewed InfoSec policies were documented in Table 4.8.

Table 4.8: Thematic grouping of policy problems to develop themes

<table>
<tr><th colspan="3">Semantic/Lexical ambiguity</th></tr>
<tr><th>Document name</th><th>Statement</th><th>Problem</th></tr>
<tr><td>P1</td><td>5.6. “Users will not collect, maintain, use or disclose personal information for personal or illegal purposes”</td><td>It is confusing that personal information should not be used for personal purposes.
Simply, the user should read the statement and interpret it relative to the definition of personal information provided. In addition, it is not clear if one should not use one’s own personal information as well or only that of others.</td></tr>
<tr><td>P6</td><td>7.4. “All communication and/or communication related information collected through interception and /or monitoring will be destroyed within four years from the date upon which it wa/s collected”</td><td>Says only “within four years”; does not give the minimum period for which the information will be kept. Therefore, the period range could be anything from a day to four years.</td></tr>
<tr><th colspan="3">Vague/Implicit description</th></tr>
<tr><td>OP1</td><td>8. “This includes creating difficult-to-guess computer passwords”</td><td>What do they mean by “difficult-to-guess”? The policy should define password requirements for its complexity, length and strength.</td></tr>
</table>

OP1	9. “You must destroy or render unusable any confidential or highly confidential information contained in any physical document”	The document does not say how to destroy or render unusable (assumes prior knowledge).
P1	8.2. “Unisa will, as far as reasonably possible, provide employees with the necessary tools and guidelines to provide basic online privacy features such as tools to detect and destroy spyware located on employees’ work stations”	How are these provided?
P7	5.6. “Heads of operational units are responsible for: informing the students of this Policy and taking appropriate action when students do not adhere to the guidelines for acceptable use”	What are the operational units? The role is vague.
P7	16.2.4. “Email messages should be kept brief and should be formulated appropriately”	What do they mean by “brief”? Up to how many words? Moreover, what is appropriate formulation of an e-mail? Do the users know?
P3	8.1.4. “A user must ensure that a mobile device is reasonably secured when on and off the campus”	What exactly is meant by “reasonably secured”?
P5	10. “Proper internal control is to be maintained over all ICT assets, at all times. Proper ICT asset management – from requisition to disposal – ensures a much greater likelihood that the university will continue to meet customer	What constitutes “proper internal control”?

	requirements into the indefinite future by planning in an orderly fashion and mandating consistency throughout the university”	
P5	12.1. “Access rights to secure areas must be regularly reviewed and updated”	How often or regular is “regularly”?
	13.2. “a) … Records must be kept, for a reasonable period, of all network-based communication with both internal and external parties”	How long is “a reasonable period”?
	13.5. “All electronic information must be backed up onto secure storage media on a regular basis, for the purposes of disaster recovery and business continuity”	How often or regular is “on a regular basis”? How frequent would that be?
P2	15.1. “Employees should connect their computers on the university’s network on a regular basis to ensure that virus protection, software versions and other security patches are updated”	How often is “on a regular basis”? A minimum period should be recommended.
OP2	3.6.1.9. “All external doors and windows must be closed and locked at the end of the work day”	What about the internal office doors?
	3.10.3.1. “The IT security manager should be familiar with simple routines for collecting evidence”	Vague. What constitutes “simple routines” and what evidence would they be collecting?

Omission/Null pointer		
P6	5.8 “On application by a privacy subject, Unisa will disclose: 5.8.1. private information the institution collected from the privacy subject; 5.8.2. the purpose the information was collected for; 5.8.3 how the information was used; and 5.8.4. how the information was disclosed, if at all”	There is no indication of disclosing how the information was stored. Storage is a crucial aspect of personal information in order to ensure privacy and security; the storage of personal information has to be appropriate for its classification. Are there any minimum requirements in terms of encryption or protection of personal information in storage?
	Sections 7.1.3 and 7.2 are non-existent.	6.1.3 refers to paragraph 7.2, which is not in the document. 6.2. and 6.3 refer to paragraph 7.1.3, which does not exist. Paragraph 7 has no sub-sections.
P2	Find document “Policy on the Management of Property, Plant and Equipment”	Document not listed with IT policies on intranet.
P3	9.1.5.b) “Personally owned mobile devices connecting to the network must meet the minimum security standards prescribed by the Department: ICT”	What are these minimum standards and where are they documented/accessible?
P8	7.3. “Academic messages must adhere to the basic guidelines”	Where are the basic guidelines documented? Where are they located?

Double negative		
P2	8.2. “No item may be disposed of without the explicit approval of the ICT Disposal Committee”	The word “item” is not defined in the policy. Does it refer to ICT assets?
P5	8. “… It is unacceptable for anyone to use information resources to violate any law or Unisa policy or perform unethical academic or business acts”	The statement could be stated to indicate that users should not use the resources to violate laws or Unisa policy, instead of saying it is unacceptable. What do they mean by “unacceptable”? The policy document should state the recommended actions and not merely the attitude towards the undesired actions. What actions is the statement recommending?
OP1	Page 15: “computers should be configured to time out after no more than 20 minutes of inactivity”	Vague- double negative.
Contextual		
OP1	Section 8: physical security requirements listed with ICT security requirements	Physical security requirements listed with ICT security requirements.

While reviewing the policy documents to derive themes, some of the ambiguous words and phrases in Table 4.8, were noted to require simple one-step solutions as discussed in the next section.

4.3.1.1.Ambiguities that could be resolved in one step

The following list of ambiguous words requires a definition of what they are, in order to resolve their ambiguity:

1. Sensitive information
2. Personal information
3. Personal or illegal purposes
4. No *item* may be disposed of without …
5. Minimum security standards
6. Academic messages must adhere to the basic guidelines
7. Unacceptable
8. Sensitive information
9. Critical characteristics of information
10. Critical assets

The previous list of ambiguous words, once given a definition within the InfoSec policy document, their intended meaning ought to become evident and clear to the policy users. The policy writers should ask the question, "how" should this process be executed? Then they would be able to provide clarity on the following ambiguous phrases noted in the policies:

1. Simple routines for collecting evidence
2. Difficult-to-guess computer passwords
3. Destroy or render unusable
4. As far as reasonably possible
5. Taking appropriate action
6. Kept brief
7. Formulated appropriately
8. Reasonably secured

9. Planning in an orderly fashion
10. Proper internal control
11. Mandating consistency
12. Simple routines for collecting evidence
13. Private information
14. Safe and secure handling of information
15. Kept current
16. Properly maintained

With the above list of phrases, their related process should be clarified for their meaning to be clear. In the next list of ambiguous phrases, the time period or range should be stated in order to clarify the meaning of the words and reduce their ambiguity. The ambiguous phrases requiring a period range are:

1. A reasonable period
2. Must be backed up onto secure storage media on a regular basis
3. Regularly reviewed and updated
4. Employees should connect their computers on the university's network on a regular basis
5. No more than 20 minutes
6. Periodic reviews

Once the time period is stipulated, the meaning of the phrases should become clear to the policy users. The next list presents ambiguous phrases noted in the reviewed policies, where the words indicate assumed shared meaning or an implicit common understanding between the policy users and the policy writers:

1. Precise yet enforceable

2. Consistent
3. Easy to use
4. Have little excuse
5. Effective
6. Effectiveness
7. Effective security policies
8. Visibility
9. Awareness
10. Understanding
11. Properly educating staff
12. Higher levels
13. Behaviour for compliance
14. A nuisance
15. Compliance
16. Employee attitude
17. Human aspects
18. Social engineering
19. Malicious insiders
20. Employees’ errors
21. User awareness and education
22. Administrative security defences

Subsequent to the initial content analysis where themes were derived a secondary content analysis was performed as noted next.

For the secondary content analysis, AtlasTi software was used for a further analysis of the purposeful sample of the collected data, P1-P10. As a recap, the data were collected in the form of ICT policy documents. The documents were collected from a higher education institution in South Africa as a convenient sample. This particular institution was used, as it has ten different policies related to ICT. In general, other institutions have one InfoSec policy with sub-sections addressing other ICT aspects. AtlasTi qualitative data analysis software was used to generate the most frequently occurring words as observed across all ten policy documents. The words are documented in Figure 4.1.

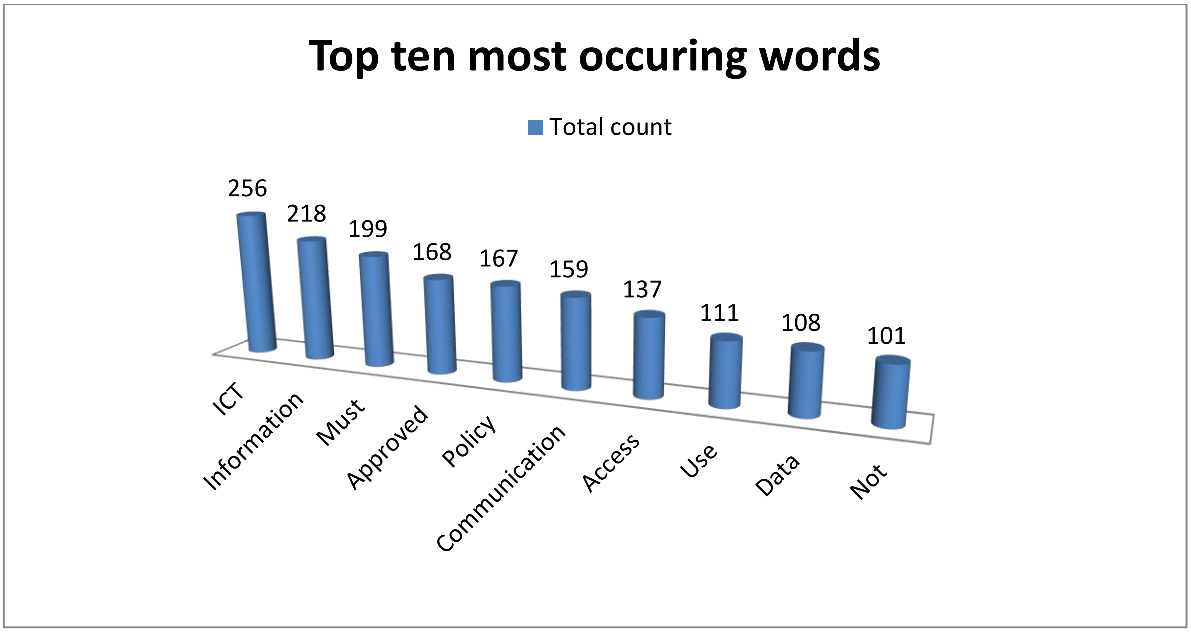


Figure 4.1: Top ten most occurring words by combined totals (generated by researcher on AtlasTi)

Only the sampled InfoSec policies from the chosen higher education institution were reviewed using the AtlasTi qualitative data analysis software. Using AtlasTi, for the secondary content analysis process, the ambiguity themes from the initial manual content analysis were used as themes for coding the data. Seventeen ambiguous statements were identified in the reviewed InfoSec policies. The results of this process are depicted diagrammatically (semantic layout) in Table 4.9.

Table 4.9: List of ambiguous words as resulting from the AtlasTi software qualitative analysis

Network view: Final semantic layout of ambiguous words
Created by: Super 2017-02-17 T22:36:12
Nodes count: 18 **Codes (1):** **Ambiguous words {17-0}** **Quotations [pdf] (17):** **1:8 the necessary tools and guidelines... (5:232-5:267)** **1:9 provide basic online privacy… (5:272-5:309)** **1:10 disclose personal information ... (3:1618-3:1683)** **2:2 item (3:1214-3:1218)** **3:2 reasonably secured (5:439-5:456)** **3:4 minimum security standards (5:2281-5:2309)** **5:3 Proper ICT asset management (4:2777-4:2805)** **5:4 Proper internal control (4:2698-4:2720)** **5:6 regularly reviewed (5:1373-5:1390)** **5:7 Logging of external communication... (8:1166-8:1325)** **5:8 reasonable period (8:1230-8:1246)** **5:10 on a regular basis (9:1558-9:1577)** **5:12 must be kept to a minimum (11:738-11:762)** **6:3 will be destroyed within four ... (7:237-7:271)** **7:2 taking appropriate action (4:1931-4:1956)** **7:4 kept brief (10:1359-10:1368)** **8:2 basic guidelines (4:1719-4:1734)**

The AtlasTi software was used to code the ambiguous phrases. Table 4.9 presents the list of identified words. The numbers in brackets indicate the location of the words in their respective documents. For example, the first ambiguous word or quotation was identified in Document P5 from letter number 232 to letter number 267 in the document, as indicated by the number (5:232–5:267). There were 18 nodes in total, as this included the heading node “Ambiguous words”.

The results of this process were also depicted diagrammatically in Figure 4.2 in the form of an AtlasTi semantic layout diagram.

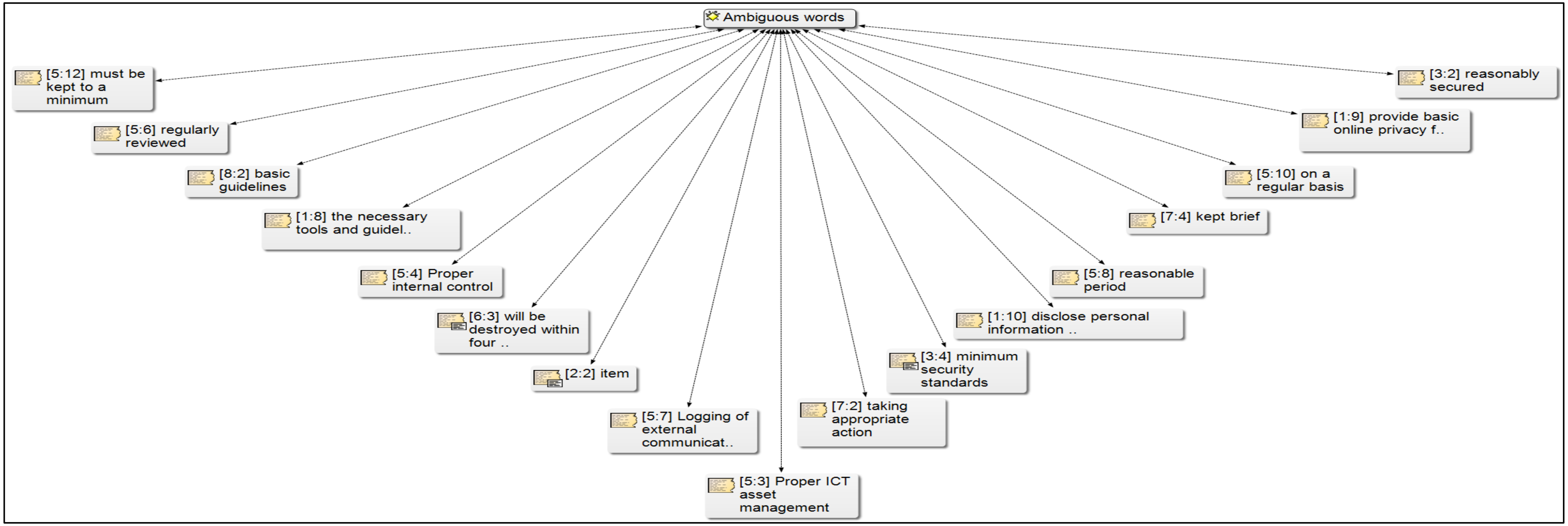

Ambiguous words
[5:12] must be kept to a minimum
[3:2] reasonably secured
[5:6] regularly reviewed
[1:9] provide basic online privacy f..
[8:2] basic guidelines
[5:10] on a regular basis
[1:8] the necessary tools and guidel..
[7:4] kept brief
[5:4] Proper internal control
[5:8] reasonable period
[6:3] will be destroyed within four ..
[1:10] disclose personal information ..
[2:2] item
[3:4] minimum security standards
[5:7] Logging of external communicat..
[7:2] taking appropriate action
[5:3] Proper ICT asset management

Figure 4.2: AtlasTi: Semantic layout of ambiguous words (generated by researcher on AtlasTi)

The semantic layout in Figure 4.2 reflects the words identified as ambiguous in the ten reviewed policy documents, P1-P10. The words are noted in their context for clarity and ease of reference. The identified ambiguous statements from the rest of the sample were grouped into their respective ambiguity themes. The themes were derived from the initial manual content analysis. The resulting categorised ambiguous phrases are presented in Table 4.10, with the ambiguous key-words and key-phrases indicated in bold text formatting.

Table 4.10: Thematically categorised ambiguous words and phrases / Results of the document review indicating ambiguous statements

Theme/ Code	**Content analysis results**		
	Ambiguous statement	**Problem description**	**Policy**
DN &VID	"**No item** may be disposed of **without** the explicit approval of the ICT Disposal Committee."	The word "item" is not defined in the policy. Does it refer to ICT assets? The statement is also phrased with a double negative.	**P2**
VID	"A user must ensure that a mobile device is **reasonably secured** when on and off the campus."	How does one ensure that a mobile device is "reasonably" secured? The policy did not provide any process steps or suggestions.	**P3**
	"The Institution will, as for as reasonably possible, provide employees with **the necessary tools and guidelines** to **provide basic online privacy features** such as tools to detect and destroy spyware located on employees' work stations."	The policy document does not define these tools and guidelines. How does the institution determine what constitutes "necessary" tools and guidelines? The document does not define what these basic features are.	**P1**
	Proper ICT asset management – from requisition to disposal – ensures a much greater likelihood that the university will continue to meet customer requirements into the indefinite future by planning in an orderly fashion and mandating consistency throughout the university."	What constitutes "proper ICT asset management"?	**P2**

	“**Proper internal control** is to be maintained over all ICT assets, at all times.”	What constitutes “proper internal control”?	**P2**
	“… Access rights to secure areas must be **regularly reviewed** and updated.”	How often or regular is “regularly”?	**P3**
	“The following logging must be implemented: a) **Logging of external communications**”	Does this statement apply to all or only some external communications? If some, which ones?	**P6**
	“… Records must be kept, for **a reasonable period**, of all network-based communication with both internal and external parties.”	How long is a “reasonable” period?	**P5**
	All electronic information must be backed up onto secure storage media **on a regular basis**, for the purposes of disaster recovery and business continuity.”	How often or regular is “on a regular basis”? How frequent would that be?	**P5**
VID	… The number of privileged accounts **must be kept to a minimum**, and only provided to those employees whose job duties require it …”	A minimum of how many? Based on what? What if 1 000 employees’ job duties require it?	**P5**
	“Heads of operational units are responsible for: informing the students of this Policy and **taking appropriate action** when students do not adhere to the guidelines for acceptable use.”	What constitutes “appropriate” action?	**P7**
	“Email messages should be **kept brief** and should be formulated appropriately.”	What do they mean by “brief”? Up to how many words? Moreover, what is appropriate formulation of an e-mail? Do the users know? The document did not provide guidelines.	**P8**
SeLA	“Users will not collect, maintain, use or **disclose personal information** for personal or illegal purposes.”	The users should read the statement and interpret it relative to the definition of personal information provided. In addition, it is not clear if one should not	**P1**

		use one’s own personal information as well, or only that of others.	
	“All communication and/or communication related information collected through interception and/or monitoring will be **destroyed within four year**s from the date upon which it was collected.”	The phrase “within four years” does not give the minimum period for which the information will be kept. Therefore, the period range could be anything from a day to four years.	**P6**
ONP	“Personally owned mobile devices connecting to the network must meet the **minimum security standards** prescribed by the Department: ICT.”	These minimum standards were not documented anywhere in the ICT policies. What are these minimum standards and where are they documented/accessible?	**P3**
	“Academic messages must adhere to the **basic guidelines**.”	Where are the basic guidelines documented? Where are they located? They were not noted in the reviewed InfoSec Policy and its sub-policies.	**P8**

The content analysis results in Table 4.10 were further presented in a pie chart, in order to highlight the distribution and prevalence of each ambiguity theme. The pie chart is presented in Figure 4.3. The graph indicates that the CON theme had no occurrences in the reviewed documents, as noted in Figure 4.3, with 0%. There was a 6% occurrence of the DN theme. There was therefore a low significance of ambiguities occurring because of double negatively phrased statements.

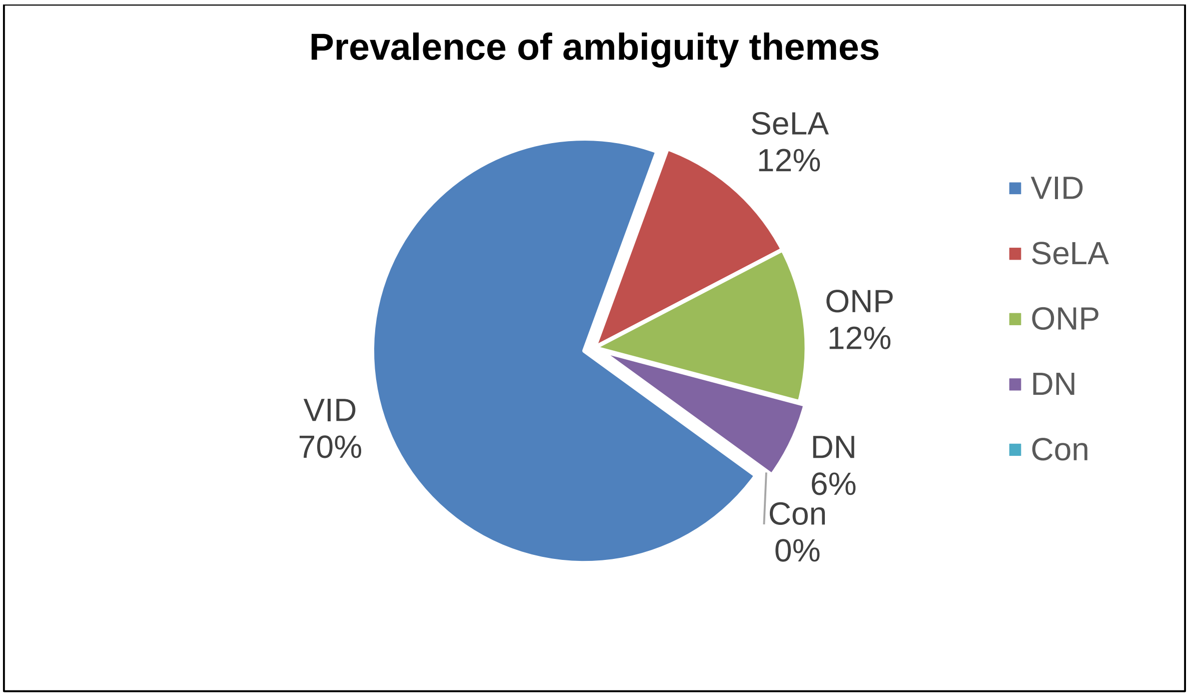
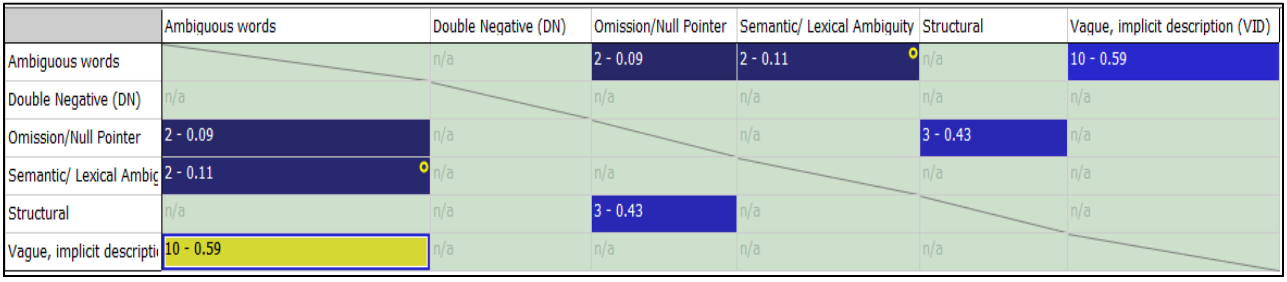


Figure 4.3: Thematic occurrences of ambiguous phrases / Distribution of the problem categories

Both the ONP and the SeLA themes had minimal occurrences at 12% of the ambiguities each, together accounting for a mere 24% of all occurring ambiguities. The VID theme, on the other hand, had the most occurrences, accounting for 70% of all identified ambiguities.

The data were further analysed in AtlasTi for co-occurrences. A co-occurrence indicates associations between concepts. In the case where codes are co-occurring, it means that they are coding the same quotation or they are coding quotations that are touching each other in some manner per table 4.11, e.g. overlapping.

Table 4.11: Co-occurrences of ambiguity



	Ambiguous words	Double Negative (DN)	Omission/Null Pointer	Semantic/ Lexical Ambiguity	Structural	Vague, implicit description (VID)
Ambiguous words		n/a	2 - 0.09	2 - 0.11	n/a	10 - 0.59
Double Negative (DN)	n/a		n/a	n/a	n/a	n/a
Omission/Null Pointer	2 - 0.09	n/a		n/a	3 - 0.43	n/a
Semantic/ Lexical Ambic	2 - 0.11	n/a	n/a		n/a	n/a
Structural	n/a	n/a	3 - 0.43	n/a		n/a
Vague, implicit descripti	10 - 0.59	n/a	n/a	n/a	n/a	

The co-occurrence table, table 4.11, indicates the intensity of the co-occurrences measured by the C-coefficient, whose values range between 0 and 1. The "Ambiguous words", variable co-occurs with the omission variable. This is due to the fact that omissions are categorised as a form of ambiguity, as it is not clear where the user should refer to for that particular statement. "Ambiguous words" also co-occur with semantic ambiguity and vague implicit descriptions, as it is a subset of these types of ambiguities. Because they have the language theme in common. As noted in table 4.11, the Contextual(CON) theme was initially called St (structural) and later changed to CON.

From the co-occurrences, it was noted that there were commonly occurring sub-themes within the SeLA, DN and VID themes, such as:

- *Language*: The use of unclear language by the policy writers;
- *Knowledge*: assumed background knowledge of the policy user by the policy writers; the knowledge type could be
    - *Educational knowledge;*
    - *InfoSec awareness knowledge;*
    - *Experience/experiential knowledge;*
        - *Personal experience in technology use;*
        - *Organisational culture and practices*;

Similarly, there were commonly occurring sub-themes between the ONP and Con themes such as:

- *Structure*: the manner in which the InfoSec policy is laid out.
- *Relation*: how the different sections and aspects of the policy relate to and reference each other.

For this reason, the SeLA, DN and VID themes were grouped into the *Language* sub-theme; while the ONP and Con themes were grouped into the *Structure* theme. These groupings were conducted on the content analysis results of the data from the purposive sample. I.e. P1-P10. From this analysis, the population distribution was represented in Figure 4.4.

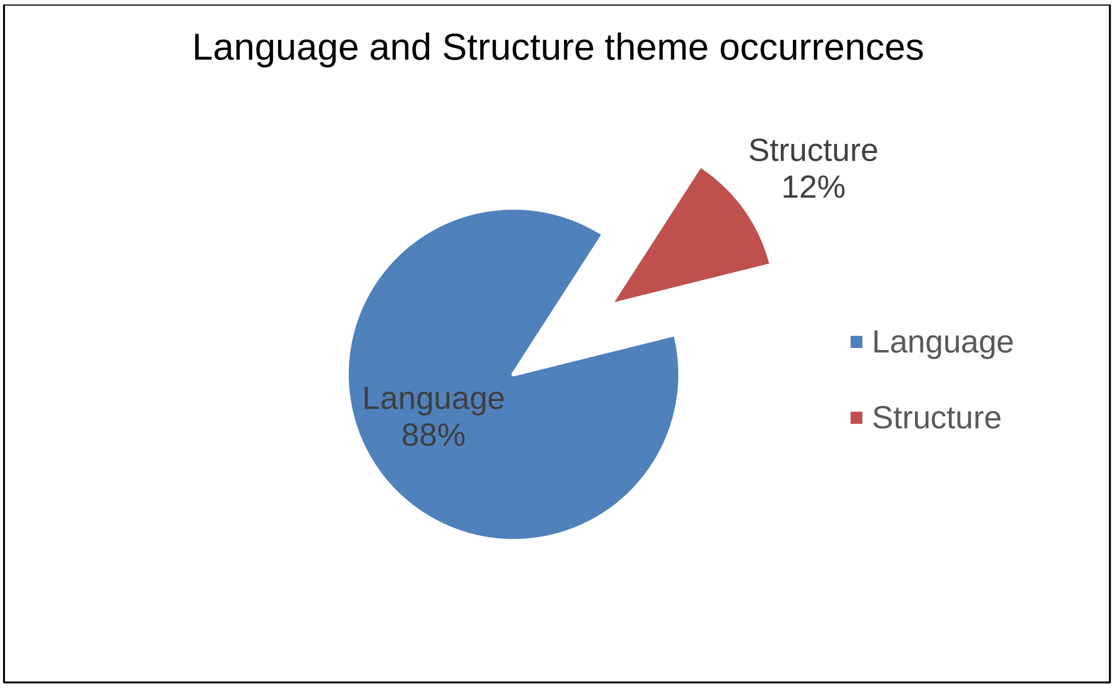


Figure 4.4: Population distribution of the “language” and “structure” themes

Figure 4.4 reflects the occurrence of the language theme and the structure theme relative to each other. The most prevalent theme was the language theme at 88 % of the ambiguities. The structure theme accounted for only 12% of the ambiguity occurrence.

Similarly, “omissions” co-occurs with structural ambiguity because it is a subset thereof. Omissions indicate the missing document references and the structural category highlights that either statements or documents referred to are not provided or they do not exist.

4.4. Conclusion

The VID category, having the most number of statements, suggests that most of the policy statements in the reviewed policies were ambiguous due to their implicit nature. The implicit documentation of the InfoSec policies suggests the possibility of assumed user background knowledge by the policy writers, having made assumptions about the reader’s prior contextual InfoSec knowledge or experience. Clearer policy statements with simpler structure could increase compliance.

The fourth research objective of defining how InfoSec policy ambiguity can be reduced in order to improve compliance and clarity, was addressed by means of the proposed solutions and framework in the next chapter, Chapter 5. The proposed solutions and framework are represented in the form of model building and application scenarios to test the proposed frameworks.

Chapter 5
Proposed solution and Framework

5.1. Introduction

The previous chapter presented the research results and findings that emerged after applying the research methodology, and the analysis of the results. This chapter aims to shed some light on how the identified ambiguity problems could be addressed. An initial attempt at addressing the problems as identified by the study was a general review of the problem categories and what they had in common. They all lack clarity, in one way or another.

Based on the category definitions and descriptions, a general solution is suggested per category and documented in Table 5.1. This chapter further proposes some possible solutions in order to address the problems identified in the research findings of the study.

Table 5.1: General ambiguity solutions per category

Theme	SeLA	VID	ONP	DN	Con
Proposed solution	Be more specific when compiling policy statements to increase clarity and reduce the SeLA category of ambiguity.	Explicitly describe the actions that the users should perform to comply with the policy statements. Reduce the presence of implicit policy statements.	Conduct a self-review of the policy statements before the final release or update. Rewrite the policy statements to reflect the correct location of other related documents or statements. Alternatively, remove the statement if the related documents are no longer applicable or no longer relevant.	Phrase statements positively and avoid the double negative category of ambiguity. The policy statement should reflect a positive phrasing of what the users should do, and avoid introducing double negatives, unless it is the only way to get the message across. E.g.: Users should **not** leave their ICT equipment **unattended** when travelling.	Move the statement to the correct section. Alternatively, remove the statement if it is no longer relevant.

In addition to the general category solutions in Table 5.1, it is recommended that in order to generally increase policy statement clarity, each policy statement should be clear with regard to the following questions and not leave it to the user's discretion. The researcher synthesised a framework, in the form of a list of questions that the policy writers should ask, in order to facilitate that each policy statement has clearly addressed the questions of what is required from the user. The questions are depicted in Figure 5.1 and listed as follows:

- Actor: Who should carry out the action or perform the activity?
- Action: What is the action required of the user? What should the user do?
- Process: How should the process steps be carried out?
- Time: When should the action be carried out? When should the user act?
- Duration: For how long should the user carry out the action?
- Range: How much of the activity should the user do? What is the minimum or maximum?

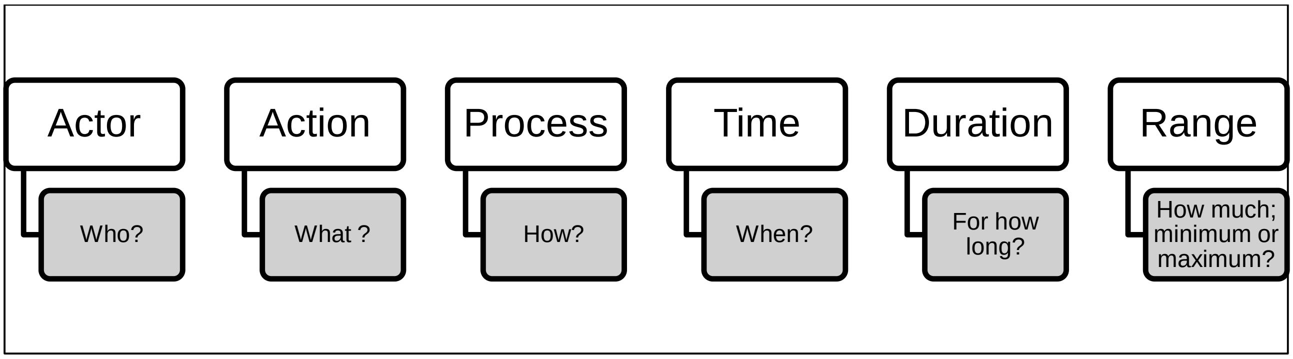


Figure 5.1. Framework of questions to probe in order to increase clarity and reduce ambiguity (synthesised by researcher)

The questions posed in Figure 5.1 should help policy writers to clarify policy statements. This method of problem solving was borrowed from UML use case diagrams where the system users, also referred to as actors, are depicted in their interactions with the system (Abdelaziz, El-Tahir & Osman, 2015; Sommerville, 2013). See Figure 5.2 for an example of a use case diagram.

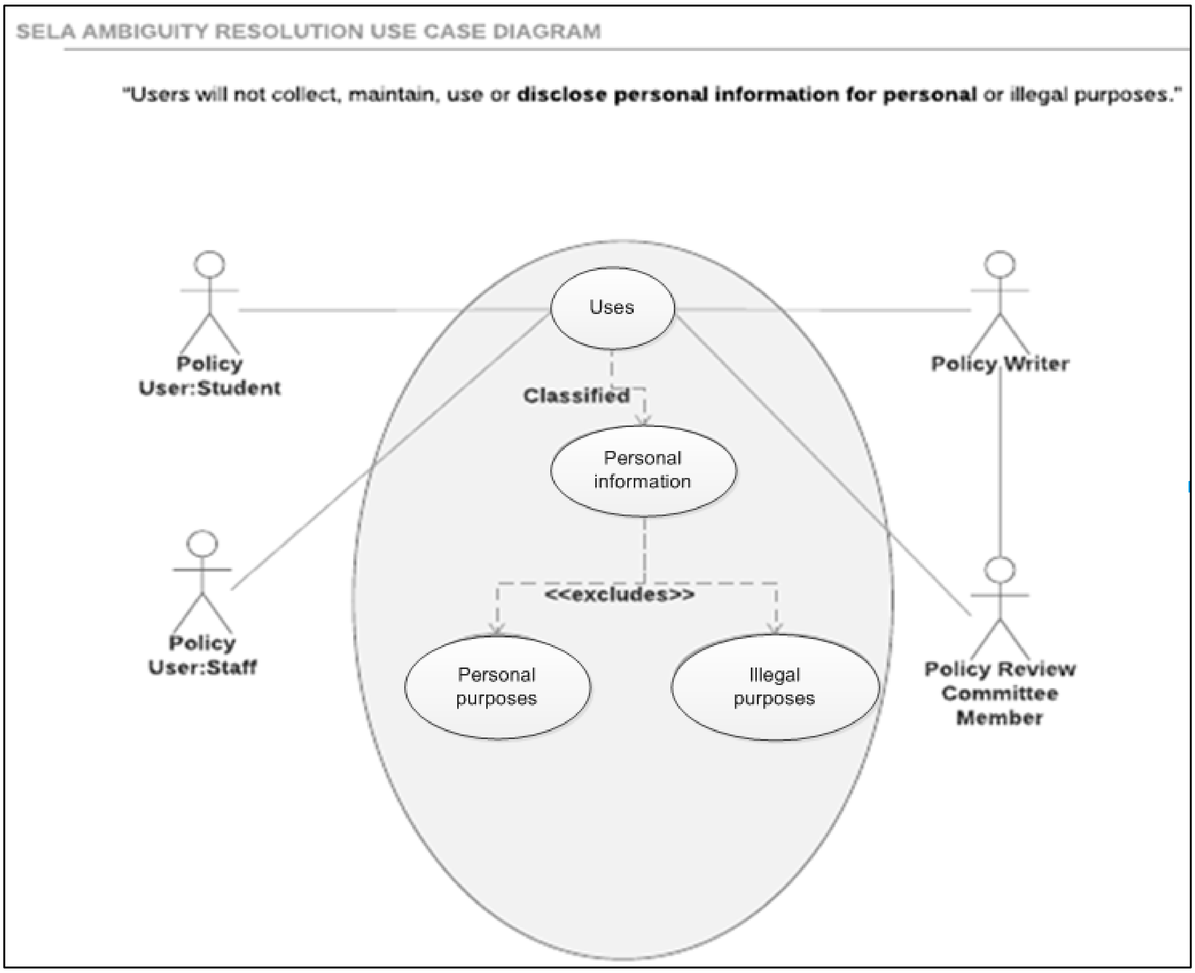

SELA AMBIGUITY RESOLUTION USE CASE DIAGRAM
"Users will not collect, maintain, use or disclose personal information for personal or illegal purposes."
Policy User:Student
Uses
Policy Writer
Classified
Personal information
Policy User:Staff
<<excludes>>
Personal purposes
Illegal purposes
Policy Review Committee Member

Figure 5.2: A use case diagram representing an ambiguous statement (synthesised by researcher)

Figure 5.2 represents a sample ambiguous statement taken from policy P1, in the SeLA theme: "*Users will not collect, maintain, use or disclose personal information for personal or illegal purposes*."

Use cases can help identify the different types of users and how they interact with the system. This aspect can assist policy writers to identify the different InfoSec actions required from the different system users, based on their interactions with the different systems. In Figure 5.2, the use case diagram indicates people or role players in the form for stick figurines labelled policy writer, policy reviewer, policy user, student and staff. In the oval, are the activities performed by the role players.

It is often said that the best way to address any problem is to break it up into smaller sections, and that is what the researcher did to further provide category-specific ambiguity solutions. This strategy was derived from the concept of "divide and conquer" made popular by Frank Capra in his 1943 propaganda film "Why We Fight: Divide and Conquer" (Frank Capra, 1943, cited in Xifra & Girona, 2012). The Frank Capra film series was made in 1943 and centred on infiltrating and the conquering the enemy (Boddy, 2011; Xifra & Girona, 2012). The divide and conquer strategy is also used in economics, politics, history as well as in sociology, and is referred to as "divide and rule" (Boddy, 2011).

There is an algorithm in computer science with the same name as the strategy, namely the divide and conquer (D&C) algorithm, which subscribes to the fundamental concepts of the D&C strategy (Dwyer, 1987). The D&C algorithm is applied by repeatedly breaking down a problem into smaller manageable chunks of the same or related type until the chunks are simple enough to be solved directly. The key strength of D&C is optimisation of resources.

In light of the D&C strategy and algorithm, the identified ambiguity problem categories were then reviewed individually in order to provide some practical solutions per category, starting with the SeLA category. The following solutions put forward.

5.2. Structural, semantic and lexical ambiguity (SeLA)

Ontologies (ontology-based interpretation of natural language) have been used in literature to address semantic ambiguity in natural language by representing the knowledge as concepts of the domain under review (Jurisica, Mylopoulos & Yu, 1999; Yarowsky, 1994).

Providing the details of the domain context for the area under discussion, has been suggested to resolve structural ambiguity. Automation has also been used for lexical ambiguity resolution. In the field of computational linguistics, statistical decision procedures are used for lexical ambiguity resolution by use of algorithms that exploit the syntactic patterns and generate a disambiguation in the target context (Yarowsky, 1994). The use of ontologies and automation software would require technical skills from policy users.

The ambiguity problem has is an age-old problem. Bunt (1984:131) reports that “[t]o some extent this ‘ambiguity explosion problem’ is an artefact of the usual method of formal semantic analysis”. He suggests the use of formal methods for dealing with ambiguity (Bunt, 1984).

As per the literature on formal methods, the FOL language was found to be among the least technical and closest to natural language (Hinchey, Bowen & Rouff, 2006). Do Amaral, Bazilio, Da Silva, Rademaker & Haeusler (2006) recommend the use of formalisation to extract the semantics of the intended action statements from security policies. This was also the intended results for this research, using a formalism that is user-friendly and enables comprehensibility and ease of implementation by the users.

Therefore, the researcher applied formal methods in the form of first-order logic to a sample ambiguous statement from the SeLA category derived from the data-analysis phase of the research process. FOL was applied to the statement as an example, and to test the usefulness of FOL in addressing the identified ambiguity:

A statement taken from policy P1, in the SeLA theme specifies: "*Users will not collect, maintain, use or disclose personal information for personal or illegal purposes*."

Applying FOL, defining the predicates, followed by the sentence give:

Predicates:

$User\ (x\ )$: x is a user.

$Personal\_info(y)$: y is someone's personal info.

$Collect(x, y)$: x collects info .

$\mathrm{Maintain}(x, y)$: x maintains info .

$\mathrm{Use}(x, y)$: x uses info .

$\mathrm{Disclose}(x, y)$: x discloses info .

$Personal\_use\ (x, y)$: x uses y for personal purposes.

$Illegal\_use(x, y)$: x uses y for illegal purposes.

FOL representation:

$(\forall x)(\forall y)(\ User\ (x)\ \land\ Personal\_info(y) \rightarrow \neg\ \ \big((Collect(x, y)\ \lor\ \mathrm{Maintain}(x, y) \lor$ $\mathrm{Use}(x, y) \lor \mathrm{Disclose}(x, y)\big)\ \land\ (\ Personal\_use\ (x, y)\ \lor\ \ Illegal\_use(x, y))\ )$ [1]

The process of translating a natural language statement to FOL is usually challenging, therefore a first step could be to first rewriting the natural language statement into a different format as follows:

Reformulation of natural language statement:

For all users, if there are personal information then such information should not be used for non-work purposes.

As before the predicates evident in the above reformulation are defined first:

$User(x)$: x is a user.
$Personal\_info(y)$: y is personal info.
$Action(x,y)$: User x takes an action on info y. The relevant actions are defined below.
$Non\_work\_use\ (x,y)$: User x uses info y for non-work purposes.

Where
Action ::= Collect | Maintain | Use | Disclose
Non_work_use::= Personal_use | Illegal_use

FOL formulation of the alternative natural language statement:

$(\forall x)\ (User(x) \rightarrow \left((\exists y)\left(Personal\_info(y) \rightarrow \neg\ (\ Action(x,y) \wedge\ Non\_work\_use(x,y))\right)\right))$ [2]

The question arises which of the two formulae are to be preferred. It turns out formula [1] is stronger than formula [2], as can readily be verified by a theorem prover, e.g. OTTER (McCune, 1994). On closer inspection, we note formula [1] makes a strong statement about **all** users (x) and **all** information (y). Hence, no user (not even a top-level manager) is allowed to perform the said action on any information for malicious purposes. In formula [2], however, the y becomes a function of x, since it is in the scope of x.

So, depending on who the user is in the organisation, it is possible the user may be allowed to manipulate the information. This is not necessarily wrong or unwanted, so the decision as to which of formula [1] or [2] to prefer, depends on who may manipulate which kind of information according to (other) organisational policies. From the OTTER theorem prover, formula [1] states the prohibited actions, whereas formula [2] seems to suggest role-based access control.

A decision tree can also be used to represent the natural language statement in order to add clarity to the FOL version of the policy statement to add clarity to the natural language statement. Subsequently, a decision tree was used to represent the structure and decision path of the statement. See Figure 5.3.

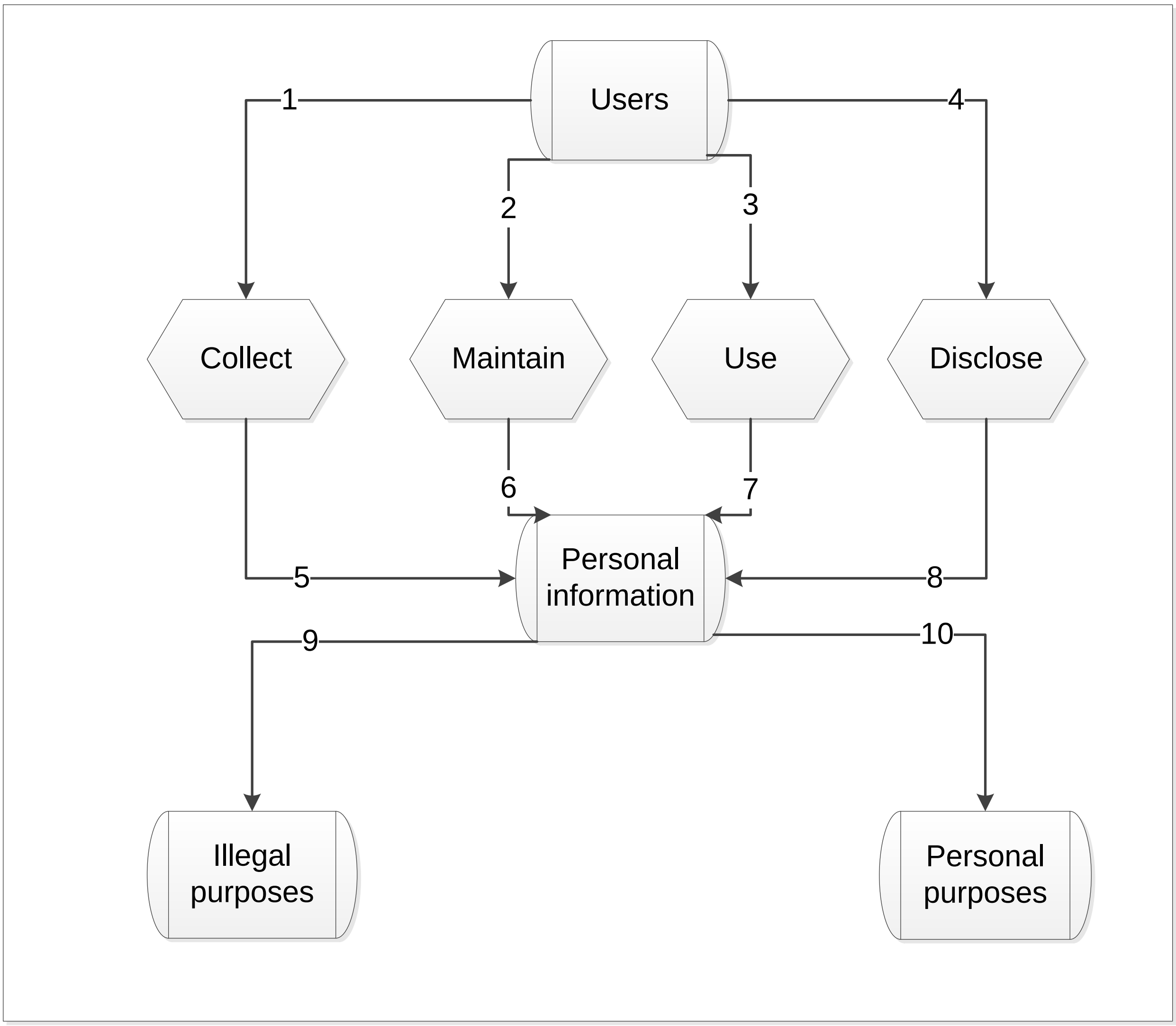


Figure 5.3: A decision tree representing a SeLA ambiguous statement with ten branches/nodes (synthesised by researcher)

In Figure 5.3 the decision tree represents the decision process for the user. Each node of the decision tree is numbered to reflect its sequence in the execution process. The decision tree may be further simplified to reduce the number of nodes in the tree from ten nodes to three nodes, as demonstrated in Figure 5.4.

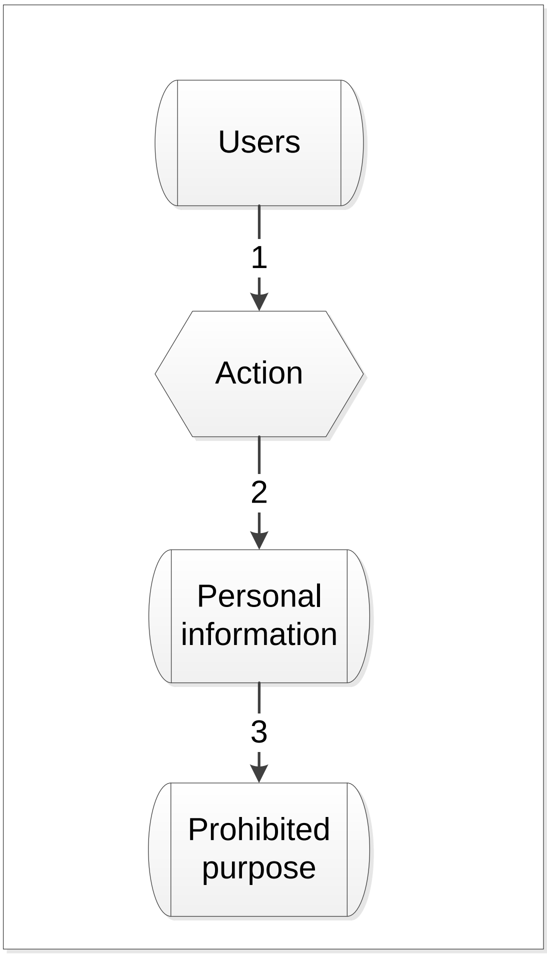


Figure 5.4: A decision tree representing a SeLA ambiguous statement with three branches/nodes (synthesised by researcher)

In order to avoid having to write ten FOL statements representing each node of Figure 5.3, and to represent it only once, the number of nodes in the decision tree were reduced. Firstly, all the actions were compressed together into a set of the elements:

Therefore, the decision tree in Figure 5.4 emerged as a result of the reduced number of nodes, with elements compressed into sets. From the decision tree in Figure 5.4, the corresponding FOL representation of the statement becomes:

Therefore: The classified information should only be used for work-related purposes, as seen in the third representation of this statement, and essentially, the formalisation process has brought to light the fact that this statement was not only SeLA but also negatively phrased.

The initial assessment had focused on double negatives as seen to cause ambiguity. However, the formalisation of the current statement has proved that negative phrasing of statements could also reduce statement ambiguity. Therefore, it is suggested by the researcher that the statement be phrased in a positive manner prior to being formalised. Thereafter, the positive paraphrased version of the policy statement would be:

““Users should collect, maintain, use, or disclose organisational classified information for work-related purposes only.”

Should the policy writers be non-technical users, any technical solutions would require them to acquire additional skills or learn a new technical language. Therefore, it accentuates the realisation that a simple type of solution would be practical and usable for the InfoSec policy owners and writers. Such a more simplistic solution is henceforth provided for each ambiguity problem category, starting with SeLA in Figure 5.5. Table 5.1 also provides an overview of the simpler solutions in the introduction of this chapter.

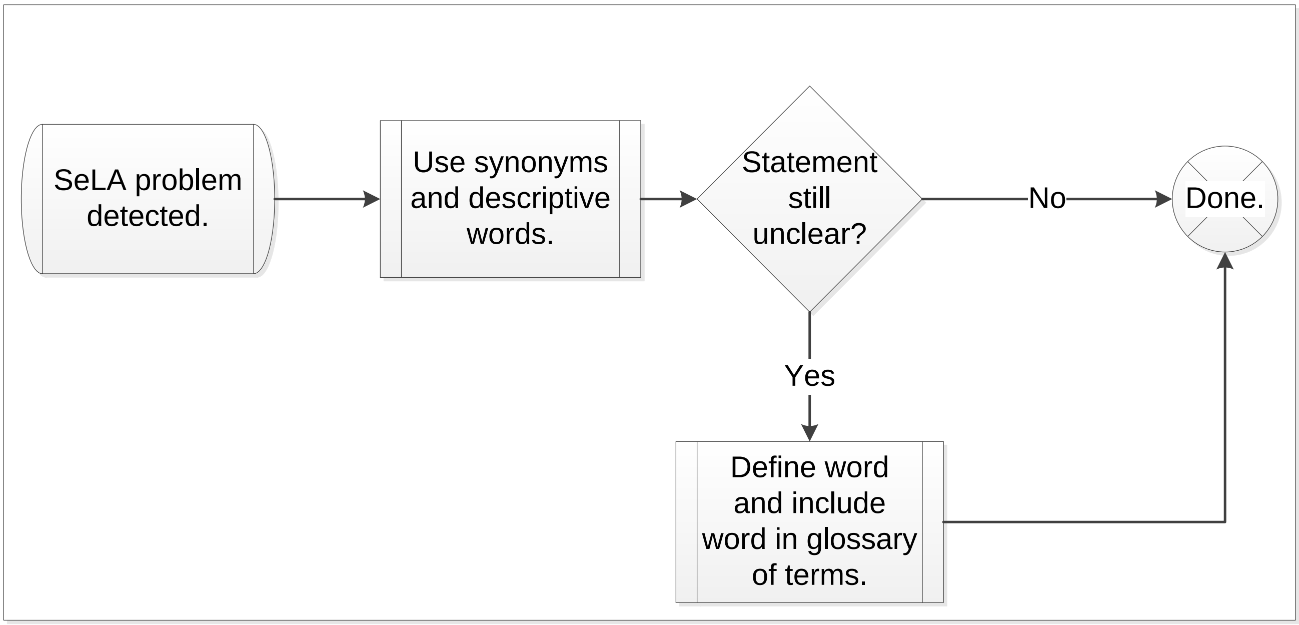

SeLA problem detected.
Use synonyms and descriptive words.
Statement still unclear?
No
Done.
Yes
Define word and include word in glossary of terms.

Figure 5.5: A general solution framework for solving SeLA problems (synthesised by researcher)

Example problem resolutions:

To test the solution provided in Figure 5.5, the following SeLA statement was used as a sample:

"Users will not collect, maintain, use or ***disclose personal information for personal*** *or illegal purposes."*

Figure 5.6 shows the process of SeLA resolution being followed to address a sample SeLA category problem. Once the process is done, the resulting disambiguated policy statement became:

"Users will not collect, maintain, use or disclose information classified as 'personal information' by the organisation, and obtained as part of their duties for non-work-related or illegal purposes."

OR

"Users will not collect, maintain, use or disclose organisational information obtained as part of their duties or classified as 'personal information' for non-work-related or illegal purposes."

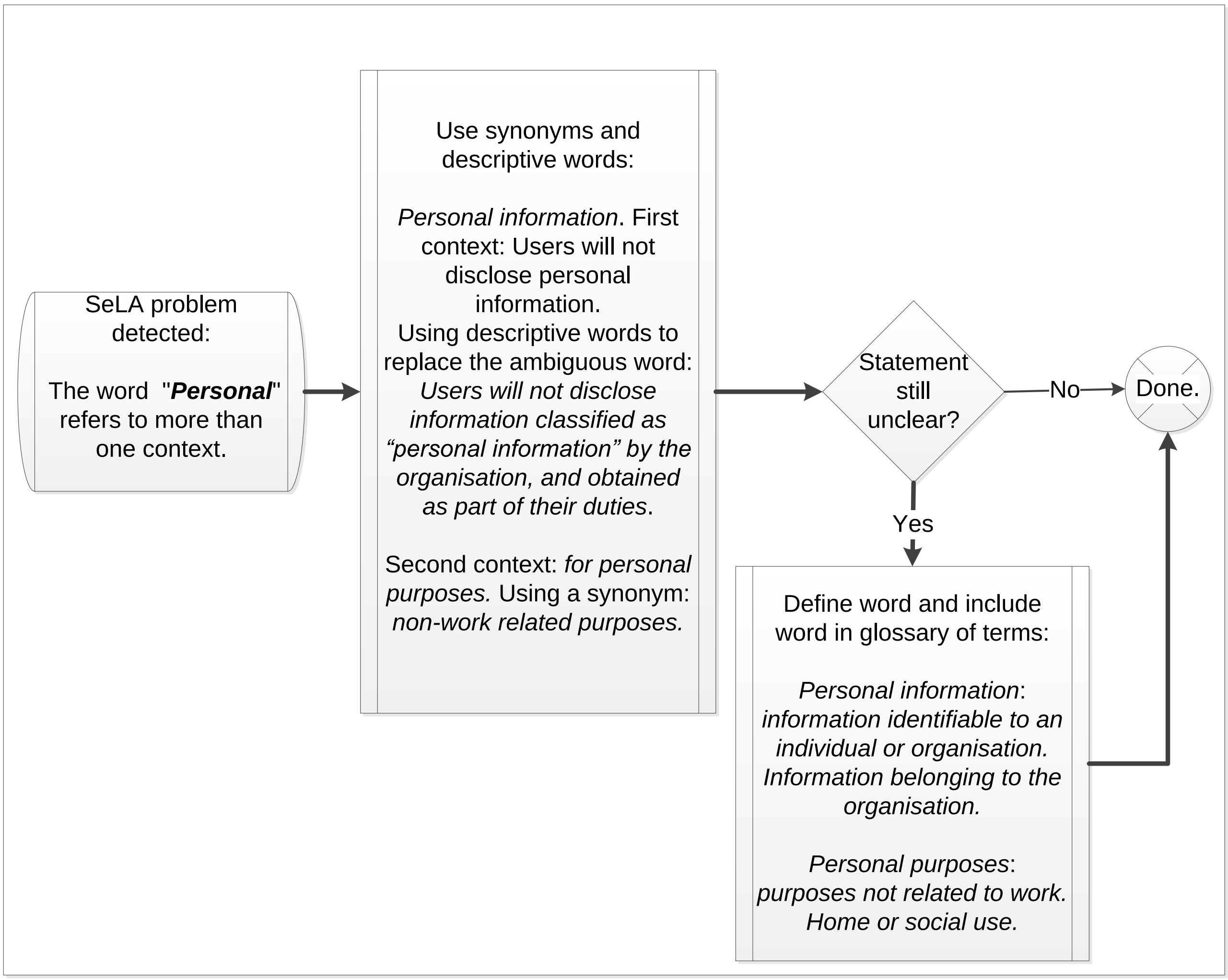

SeLA problem detected:
The word "*Personal*" refers to more than one context.
Use synonyms and descriptive words:
Personal information. First context: Users will not disclose personal information.
Using descriptive words to replace the ambiguous word: *Users will not disclose information classified as "personal information" by the organisation, and obtained as part of their duties*.
Second context: *for personal purposes.* Using a synonym: *non-work related purposes.*
Statement still unclear?
No
Done.
Yes
Define word and include word in glossary of terms:
Personal information: *information identifiable to an individual or organisation. Information belonging to the organisation.*
Personal purposes: *purposes not related to work. Home or social use.*

Figure 5.6: SeLA general solution framework applied to a sample statement (synthesised by researcher)

Having formalised the statement and tested it in the sample solution, combining the results of the two processes produced the following disambiguated statement:

“Users should collect, maintain, use or disclose organisational information obtained as part of their duties or classified as ‘personal information’, only for work-related purposes and not for non-work or illegal purposes.”

The resulting statement after applying the steps in Figure 5.6 is rather long. The policy writers could also try using short policy statements for ease of reference by users.

The next section provides the framework for the VID category of ambiguity.

5.3. Vague/Implicit description (VID)

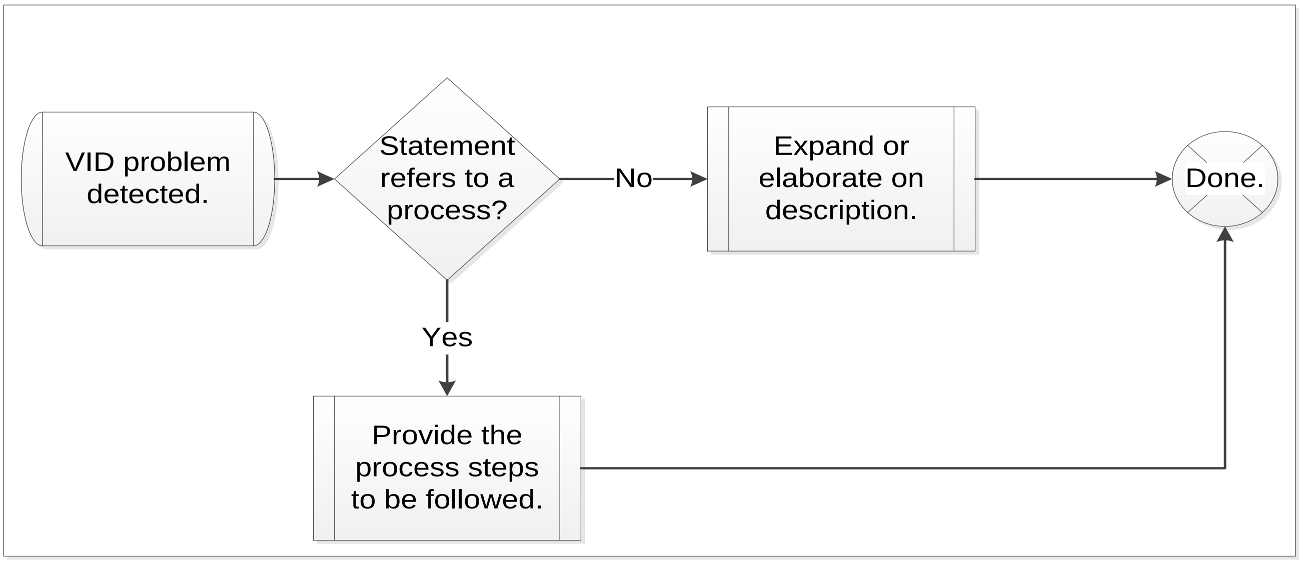
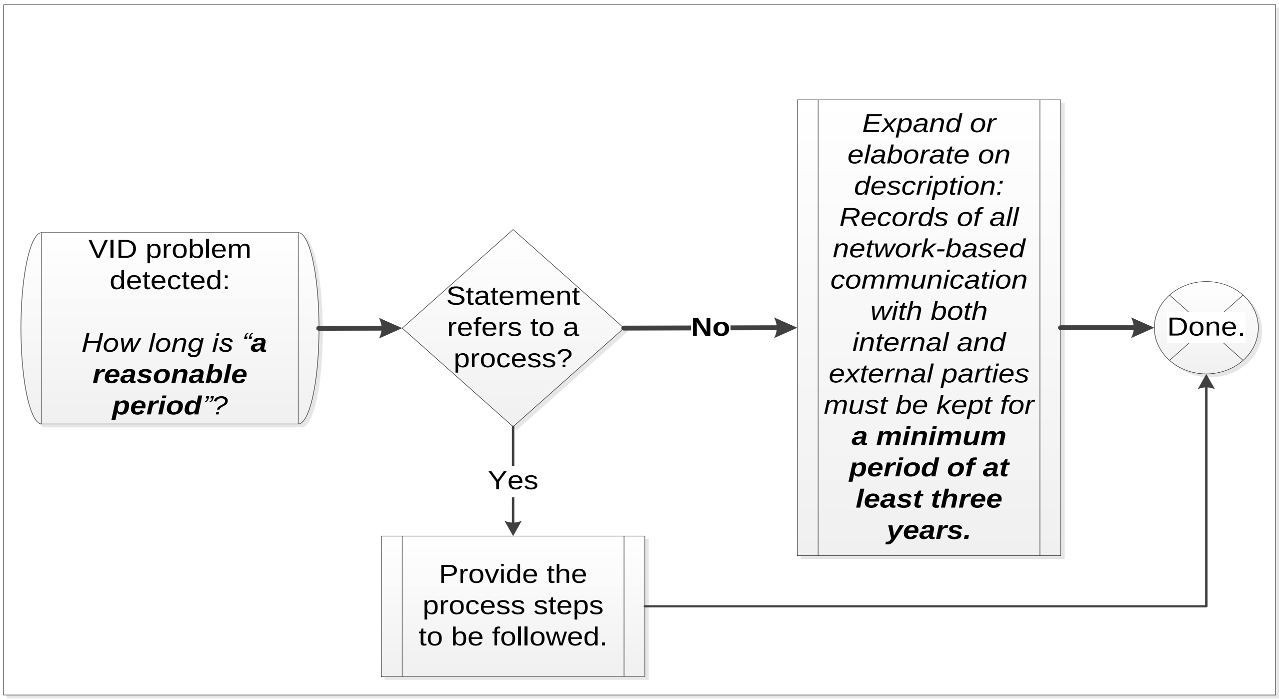

VID problem detected.
Statement refers to a process?
No
Expand or elaborate on description.
Done.
Yes
Provide the process steps to be followed.

Figure 5.7: Framework for solving VID problems (synthesised by researcher)

A policy statement from the VID category of ambiguity themes, originally taken from policy *P5* was used an example to test the proposed solution for the VID problem category. The following statement was used:

> “Records must be kept, for a *reasonable period*, of all network-based communication with both internal and external parties”.

The policy writers should define what constitutes a reasonable period. For example, choosing “three years”, as an example period. Following the VID solution steps and using three years as the reasonable period, the following solution was devised:



VID problem detected:
*How long is “**a reasonable period**”?*
Statement refers to a process?
No
Yes
*Expand or elaborate on description: Records of all network-based communication with both internal and external parties must be kept for **a minimum period of at least three years.***
Provide the process steps to be followed.
Done.

Figure 5.8: VID general solution framework applied to a sample statement (synthesised by researcher)

The revised policy statement would be:” *Records of all network-based communication with both internal and external parties must be kept for* ***at least three years.***”

The next section provides the solution framework for the ONP ambiguity theme.

5.4. Omission/Null pointer (ONP)

The framework for addressing the ONP type of ambiguity within InfoSec policy documents is presented in Figure 5.9.

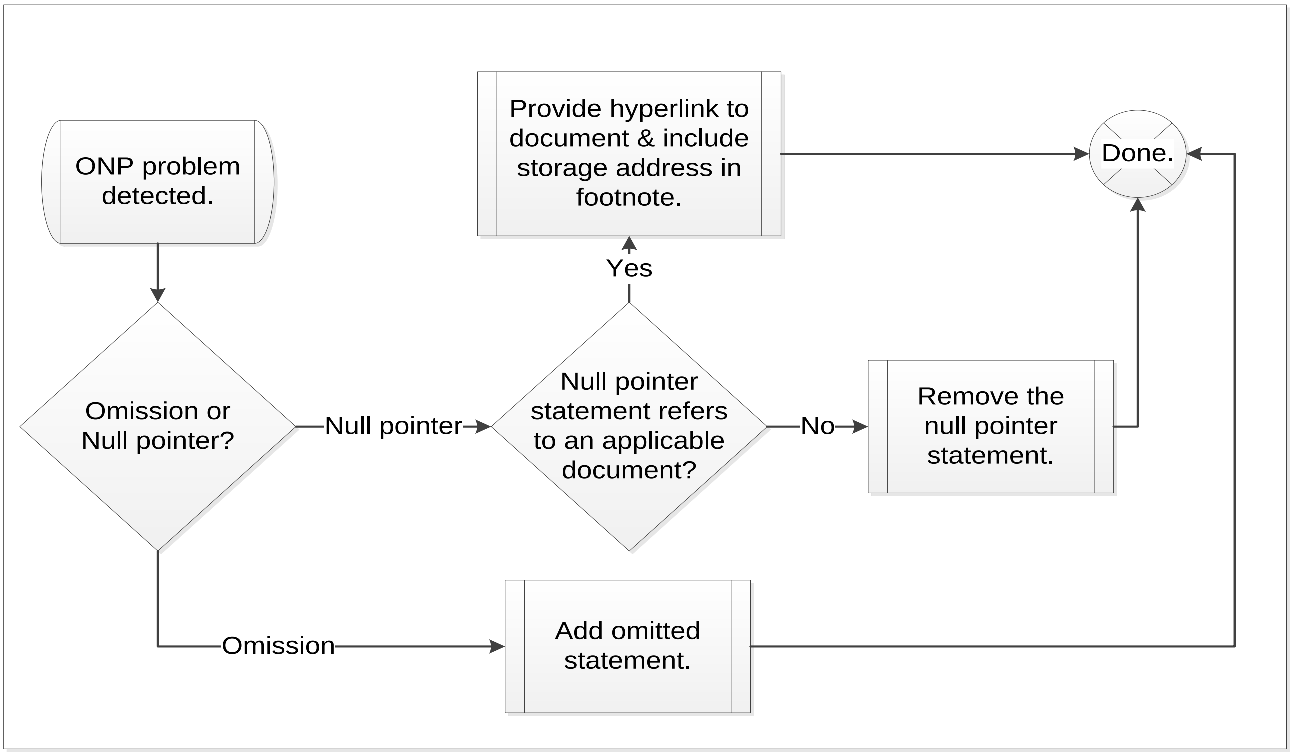
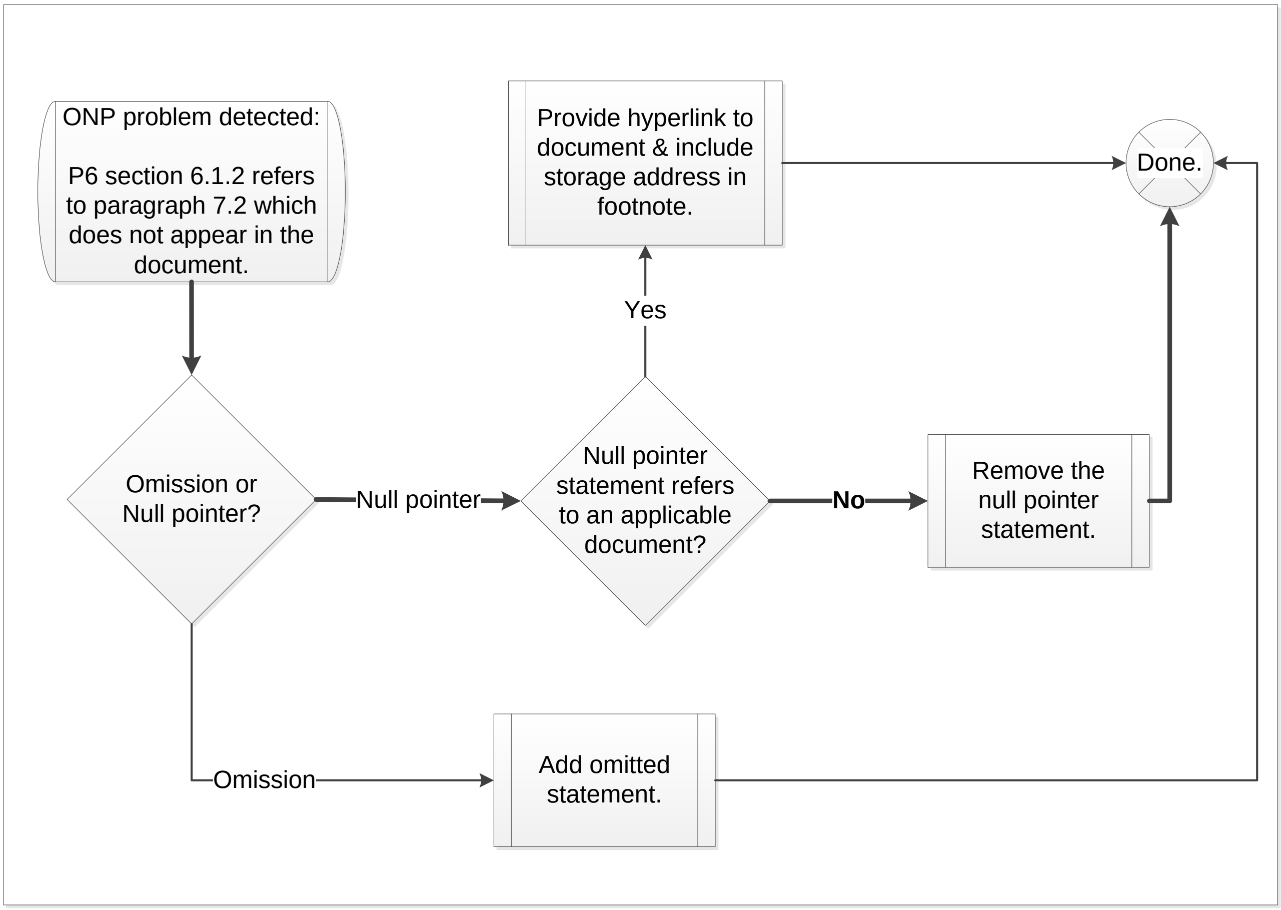

ONP problem detected.
Omission or Null pointer?
Null pointer
Null pointer statement refers to an applicable document?
Yes
Provide hyperlink to document & include storage address in footnote.
No
Remove the null pointer statement.
Omission
Add omitted statement.
Done.

Figure 5.9: Framework for solving ONP problems (synthesised by researcher)

In Figure 5.9, the framework for resolving ONP ambiguities is provided, but in order to see its usefulness, it was necessary to test it using a sample problem from the data analysis, per Figure 5.10.



ONP problem detected:
P6 section 6.1.2 refers to paragraph 7.2 which does not appear in the document.
Omission or Null pointer?
Null pointer
Null pointer statement refers to an applicable document?
Yes
Provide hyperlink to document & include storage address in footnote.
No
Remove the null pointer statement.
Done.
Omission
Add omitted statement.

Figure 5.10: ONP general solution framework applied to a sample statement (synthesised by researcher)

In the example used, section 6.1.2 of document P6 refers to paragraph 7.2, which does not exist in the document. Figure 5.10 provides an example of how this specific problem could be resolved. The next ambiguity category to be addressed was the DN (Double Negative) category as noted in the next section.

5.5. Double negative (DN)

The framework in Figure 5.11 was developed in order to address the DN types of ambiguity. The arrows in the diagram indicate the steps to be followed in the process of resolving the ambiguity.

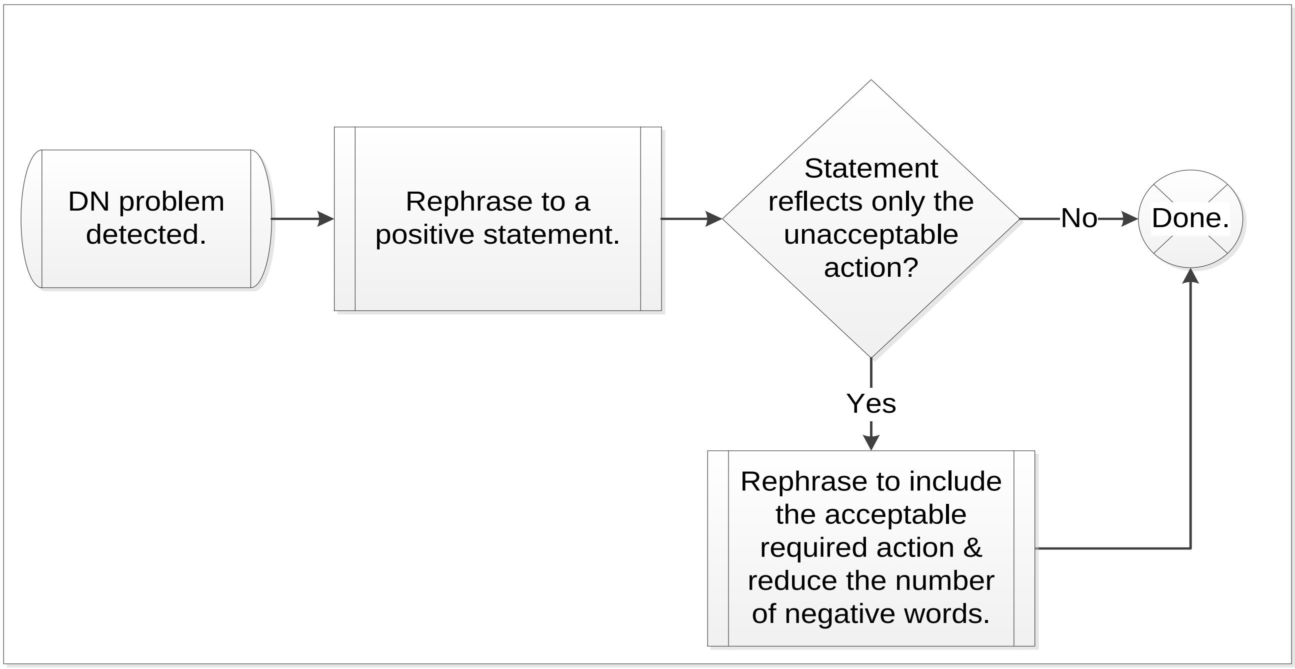

DN problem detected.
Rephrase to a positive statement.
Statement reflects only the unacceptable action?
No
Done.
Yes
Rephrase to include the acceptable required action & reduce the number of negative words.

Figure 5.11: Framework for solving DN problems (synthesised by researcher)

Figure 5.11 provides the suggested framework for DN ambiguity problems, and Figure 5.12 provides the application of this framework to an already identified problem. In order to test the framework for addressing DN types of ambiguity, a statement from policy P2, problem category, “double negative”, was used to test the proposed solution as follows:

> “No item may be disposed of without the explicit approval of the ICT disposal committee”

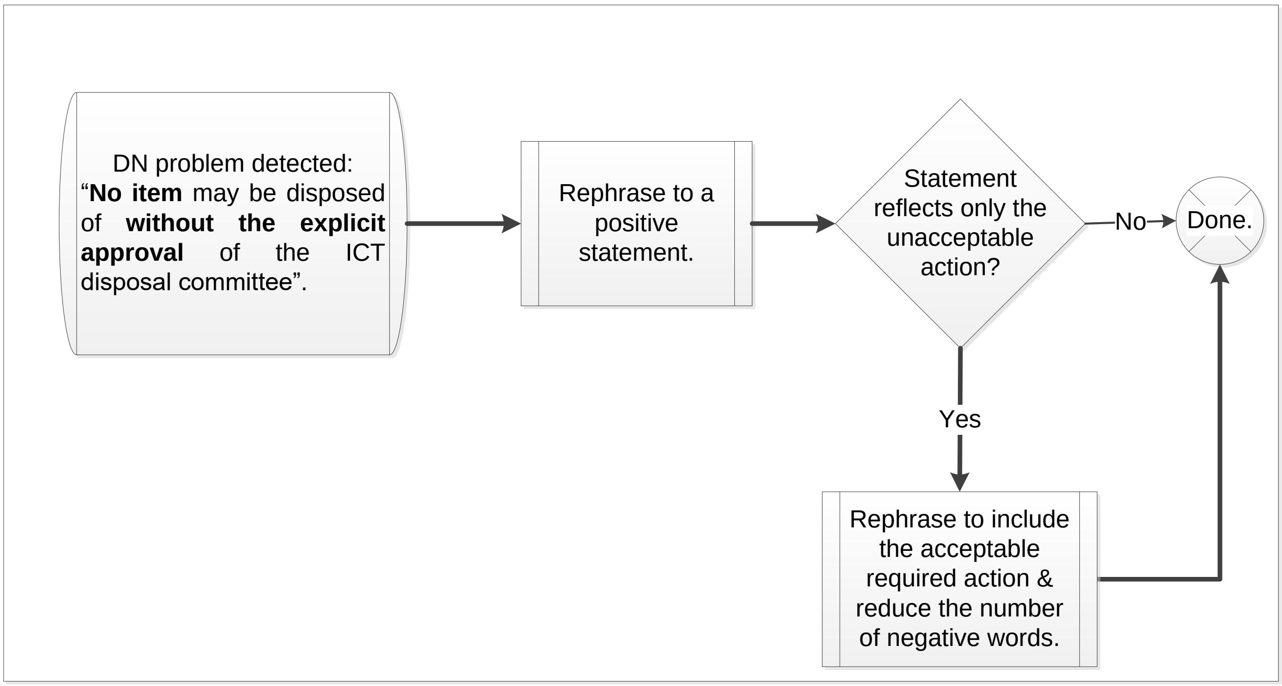

DN problem detected:
“**No item** may be disposed of **without the explicit approval** of the ICT disposal committee”.
Rephrase to a positive statement.
Statement reflects only the unacceptable action?
No
Done.
Yes
Rephrase to include the acceptable required action & reduce the number of negative words.

Figure 5.12: DN general solution framework applied to a sample statement (synthesised by researcher)

Instead of only listing what is unacceptable use as noted in Figure 5.12, the policy owners should first state what the acceptable use is. Therefore, then new statement would be:

> “The explicit approval of the ICT disposal committee should be obtained before any ICT asset may be disposed of.”

The newly phased policy statement is phrased in a positive manner for improved clarity of its intended message. The next framework addresses the Con category of ambiguity.

5.6. Contextual (CON)

The Con category of ambiguity relates to policy statements which are incorrectly placed within the InfoSec policy. These are the statements located in policy sections of an unrelated topic. The Con solution framework is presented in Figure 5.13.

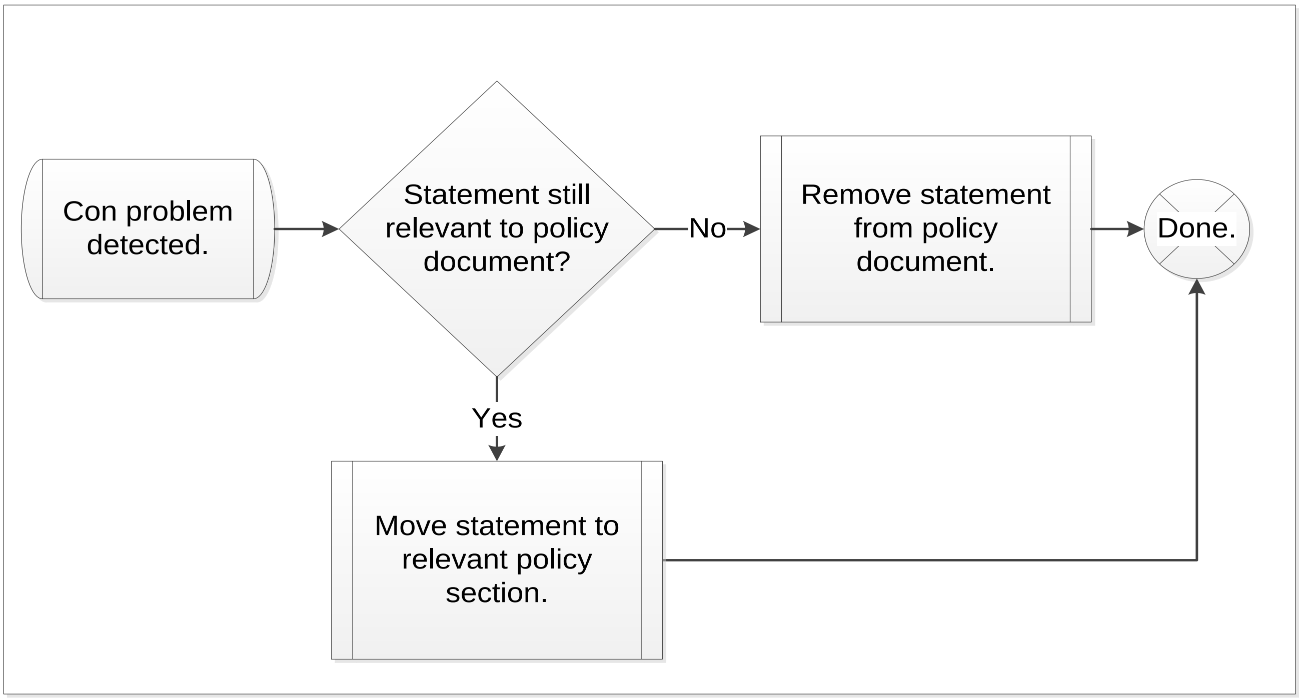

Con problem detected.
Statement still relevant to policy document?
No
Remove statement from policy document.
Done.
Yes
Move statement to relevant policy section.

Figure 5.13: Framework for solving CON problems (synthesised by researcher)

In order to test the framework in Figure 5.13, one of the online policy documents was used because the Con theme had a 0% occurrence in the purposive sample. As noted in the initial content analysis in Section 8 of policy document OP1, the document had physical security requirements listed with ICT security requirements. The testing of the Con solution framework is presented in Figure 5.14.

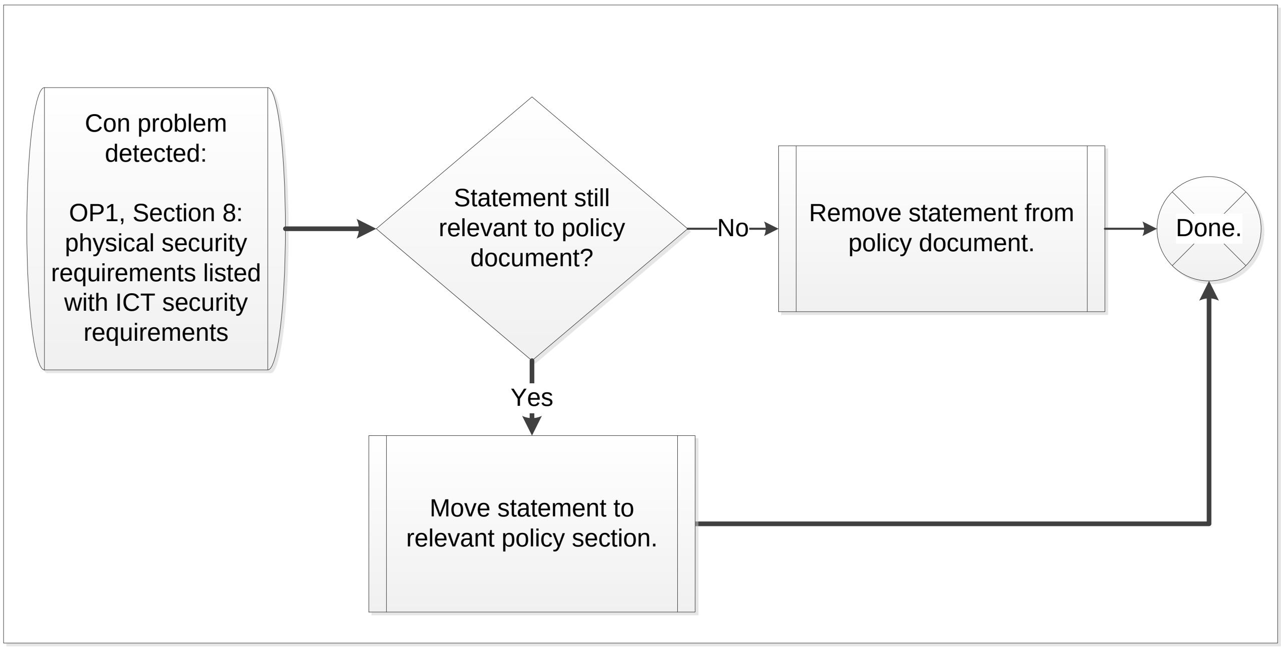

Con problem detected:
OP1, Section 8: physical security requirements listed with ICT security requirements
Statement still relevant to policy document?
No
Remove statement from policy document.
Done.
Yes
Move statement to relevant policy section.

Figure 5.14: CON general solution framework applied to a sample statement (synthesised by researcher)

With a policy statement located in an unrelated section as noted in Figure 5.14, the solution is to simply move it to the relevant policy section. The next section concludes this chapter with a chapter summary.

5.7. Chapter summary

This chapter presented the proposed solutions for reducing the identified ambiguity problems for each theme category as identified in the data analysis. The proposed solutions were provided in the form of frameworks and those frameworks were tested in a scenario format as a proof of concept. Among the solutions proposed, statements were formalised in first-order logic. The next chapter provides the recommendations and concludes the study.

Chapter 6
Conclusion and recommendations

6.1. Research overview

Chapter one: Provided an introduction to the study, the problem background, the research aims and objectives, as well as the research questions.

Chapter two: This chapter discussed the literature and related concepts underpinning the study in the form of a literature review.

Chapter three: Presented the research design and methodology, detailing the steps followed and techniques used in executing the research process, including how the data was collected and analysed.

Chapter four: Presented the research results and discussed the research findings in detail.

Chapter five: Provided the proposed solutions in the form of modelled frameworks that could be used to reduce the occurrence of ambiguity within InfoSec policy documents.

Chapter six: Concludes the study. The next section presents the summary of findings and how each research question was addressed.

6.2. Evaluation of the Study

The conclusions were drawn from the research findings of the study as guided by the researcher to address the research objectives that were presented in Chapter one to answer the research questions. The next section presents the research objectives and how they have been addressed in this study:

RO1: Explore the literature on InfoSec policies:

- The presence of Ambiguities was established within the sampled InfoSec policy documents during the content analysis process.
- The ambiguity presented itself in the form of unclear, vague and in some instances double negative policy statements. The following ambiguity categories were identified and listed, DN (double negative), CON (Contextual), ONP (Omission/ Null Pointer), SeLA (Structural/Semantic/ Lexical Ambiguity) and VID (vague implicit description).

RO2: what is being addressed- Identify the main problems InfoSec policy compliance:

- The main problems facing InfoSec policy compliance were presented in the systematic literature review section 4.2.2 as the lack of management support for InfoSec, organisational cultures of non-compliance, intentional and unintentional policy violation by employees (the insider threat), lack of policy awareness and training as well as the policy being unclear or ambiguous.

RO3: Identify the main problems affecting InfoSec policy clarity;

- The identified ambiguities posed a compliance problem as they could potentially alter the intended meaning of the policy statement to a slight variation, with unintended consequence. The policy users could misinterpret the ambiguous policy statement and act in a manner contrary to what the policy intended.

RO4: Define how InfoSec policy compliance and clarity can be improved.

- A solution framework was compiled and suggested for each identified ambiguity problem category.

The first and second research objectives, RO1 and RO2 were addressed in the form of a systematic literature review in section 4.2. The third research objective, RO3 was addressed by means of a content analysis in section 4.3. The fourth research objective was addressed by means of the proposed solutions and framework in Chapter 5.

Qualitative research methods were used to address the research objectives and answer the research questions. A case study was used in the form of the higher education institution sample, to provide an in-depth understanding of the phenomenon under study. The case study was also used to investigate a contemporary phenomenon within its real-life context (Yin, 2009). The next section presents the summary of findings from the study.

6.3. Summary of findings

This study investigated the existence of ambiguities within InfoSec policies in Higher Education and explored how the ambiguities pose a compliance problem. There were ambiguities detected in the InfoSec policies. The findings in chapter four clearly indicate that ambiguity is present and evident within InfoSec policy documents. Such ambiguity could alter the user interpretation of the policy statement.

The VID theme was the most prevalent type of ambiguity noted, and it is highly recommended that the policy writers should be aware of any assumptions that they hold about the users of their policies to avoid implicitly documenting the policy statements.

Rather, the policy writers could make a conscious effort to express the policy statements explicitly and in sufficient detail.

This study investigated the existence of ambiguities within InfoSec policies and explored how the ambiguities pose a compliance problem. There were ambiguities detected in the reviewed InfoSec policies of higher education institutions. The VID theme was the most prevalent type of ambiguity at 70%, as noted in the reviewed purposive sample of InfoSec policies belonging to a higher education institution in South Africa. It is therefore highly recommended that policy writers be aware of any assumptions they hold about the users of their policies to avoid implicitly documenting the policy statements. Rather, policy writers should make a conscious effort to express the policy statements explicitly and in sufficient detail.

In the secondary analysis, the ambiguity could ultimately be reduced into two categories, the language and structure theme. The language theme was more dominant at 88% of all observed ambiguity occurrences being accounted for in this theme. The least significant theme of structure only accounted for 12% of the overall ambiguity occurrences. Therefore, the policy writers should pay attention to their use of language in drafting the policy documents.

The Language theme included*:*

- *Language*: The use of unclear language by the policy writers;
- *Knowledge*: assumed background knowledge of the policy user by the policy writers; the knowledge type could be:
    - *Educational knowledge;*
    - *InfoSec awareness knowledge;*

- *Experience/experiential knowledge;*
    - *Personal experience in technology use;*
    - *Organisational culture and practices*;

6.4. Contributions

The results of the study should inform practice in the field of InfoSec management such that the policy writers would use the presented frameworks when drafting or reviewing their InfoSec policies, to reduce the occurrence of ambiguities. These proposed frameworks could be applied by anyone without any additional technical skills in information systems, albeit some knowledge about first-order formalisms would be needed for the underlying analysis.

The target users would be mainly, the InfoSec managers in the process of developing, reviewing, updating and maintaining the InfoSec policy document. The managers could use this study as a reference point to begin the review of their policies for ambiguities, and to address any existing ambiguities towards clearer and more enforceable policy documents. Parts of the dissertation appeared as a conference paper (Buthelezi, Van Der Poll, & Ochola, 2016).

6.5. Future work

Future research could investigate methods of resolving InfoSec policy ambiguity. User InfoSec research could borrow ambiguity resolution methods from the software development arena, which have been well researched (Abdelaziz, El-Tahir, & Osman, 2015).

The following strategies have been said to reduce ambiguity in requirements specification and could be tested for applicability to reduce ambiguity in InfoSec policies:

- Formal methods
- Ontologies
- Automated disambiguation tools such as SREE
- Manual analysis.

In conclusion, clearer policy statements, which are explicitly documented, with simpler sentence structures could increase policy clarity. Where ambiguity already exists in InfoSec policy documents, the documents could be reviewed for implicit statements and revised to reduce ambiguity and increase the clarity of the document. The increased document clarity should facilitate user compliance with the said InfoSec policy. Clearer policy statements with simpler structure could increase compliance.

6.6. Closing statement

In conclusion, clearer policy statements, which are explicitly documented, with simpler sentence structures could increase policy clarity. Where ambiguity already exists in the InfoSec policy documents, the documents could be reviewed for implicit statements and be revised to reduce ambiguity and increase the clarity of the document. The increased document clarity should facilitate user compliance with the said InfoSec policy. Clearer policy statements with simpler structure could increase compliance.

Unless InfoSec policies are designed in a way that ensures clarity, compliance may well remain a challenge. User awareness and training on the use of clear unambiguous language could be made available to policy writers in order to consciously improve the overall policy clarity.

References

Abdelaziz, A.A., El-Tahir, Y. and Osman, R. 2015. Adaptive software development for developing safety critical software. In *Computing, Control, Networking, Electronics and Embedded Systems Engineering (ICCNEEE), 2015 International Conference*. IEEE, 41–46.

Albrechtsen, E. and Hovden, J. 2010. Improving information security awareness and behaviour through dialogue, participation and collective reflection: An intervention study. *Computers & Security*, 29(4):432–445.

Almeida, J.B., Frade, M.J., Pinto, J.S. and de Sousa, S.M., 2011. *Rigorous software development: an introduction to program verification*. Springer Science & Business Media.

Andress, J., 2014. *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress.

Atlas.ti, The #1 software for Qualitative Data Analysis. Retrieved from http://atlasti.com/ [Accessed 5 March 2016].

Aveson, D. and Fitzgerald, G., 2006. Methodologies for developing information systems: A historical perspective. In *The Past and Future of Information Systems: 1976–2006 and Beyond* (pp. 27-38). Springer US.

Bandara, A.K., Lupu, E.C. and Russo, A. 2003. Using event calculus to formalise policy specification and analysis. In *Proceedings of the 4th International Workshop on Policies for Distributed Systems and Networks (POLICY'03)*. 1–14.

Baxter J. 2009. *Content analysis*. In R. Kitchin & N. Thrift (eds.). *International encyclopedia of human geography*, Vol. 1. Oxford: Elsevier, 275–280.

Boddy, C., 2011. *Corporate psychopaths: Organizational destroyers*. Springer.

Boehmer, W. 2008. Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. In *The Second International Conference on Emerging Security Information, Systems and Technologies.* IEEE, 224–231.

Blaxter, L., Hughes, C. and Tight, M. 2006. *How to research.* Third edition. Berkshire: McGraw-Hill Education.

Bowen, J.P. 1988. Formal specification in Z as a design and documentation tool. *IEEE Software Engineering*, 2:164-168

Bryman, A. and Allen, T., 2011. Education Research Methods.

Bryman, A., 2012. Social research methods: OUP Oxford.

Bryman, A. and Bell, E., 2015. *Business research methods*. Oxford University Press, USA.

Bucaria, C. 2004. Lexical and syntactic ambiguity as a source of humor: The case of newspaper headlines. *Humor*, 17(3):279–309.

Bunt, H. 1984. The resolution of quantificational ambiguity in the TENDUM system. In *Proceedings of the 10th International Conference on Computational Linguistics and 22nd annual meeting of the Association for Computational Linguistics.* Association for Computational Linguistics, 130–133.

Buthelezi, M. and Mujinga, M. 2013. Security aspects of online teaching and learning: An ODL case study. *In Proceedings of* the 2013 ICEE/ICIT. 232–241.

Buthelezi, M.P., Van Der Poll, J.A. and Ochola, E.O., 2016, December. Ambiguity as a Barrier to Information Security Policy Compliance: A Content Analysis. In *Computational Science and Computational Intelligence (CSCI), 2016 International Conference.* Las Vegas, 2016, December, pp. 1360-1367, IEEE. ISBN: 978-1-5090-5510-4.

Chang, C.Y., Wang, H.J. and Shen, W.C. 2010. Copyright-proving scheme for audio with counter-propagation neural networks. *Digital Signal Processing*, 20(4):1087–1101.

Chang, E.S. and Lin, C.S. 2007. Exploring organizational culture for information security management. *Industrial Management & Data Systems*, 107(3):438–458.

Creswell, J.W. 2009. *Research design: Qualitative, quantitative and mixed methods approaches.* Third edition. London: Sage.

Creswell, J.W., 2014. *A concise introduction to mixed methods research*. Sage Publications.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R., 2013. Future directions for behavioral information security research. *computers & security*, *32*, pp.90-101.

Dagada, R. and Eloff, M.M. 2013. Integration of policy aspects into information security issues in South African organisations. *African Journal of Business Management*, 7(31):30-69.

Danchev, D. 2003. *Building and implementing a successful information security policy*. Retrieved from *http://www.windowsecurity.com/pages/security-policy.pdf* [Accessed 12 May 2016].

Da Veiga, A. and Eloff, J.H. 2010. A framework and assessment instrument for information security culture. *Computers & Security*, 29(2):196–207.

Do Amaral, F.N., Bazilio, C., Da Silva, G.M.H., Rademaker, A. and Haeusler, E.H., 2006, October. An ontology-based approach to the formalization of information security policies. In *Enterprise Distributed Object Computing Conference Workshops, 2006. EDOCW'06. 10th IEEE International* (pp. 1-1). IEEE.

Doherty, N.F., Anastasakis, L. and Fulford, H. 2009. The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management*, 29(6):449–457.

Downe-Wamboldt, B. 1992. Content analysis: Method, applications, and issues. *Health Care for Women International*, 13(3):313–321.

Dwyer, R.A. 1987. A faster divide-and-conquer algorithm for constructing Delaunay triangulations. *Algorithmica*, 2(1–4):137–151.

D'Arcy, J., Herath, T. and Shoss, M.K., 2014. Understanding employee responses to stressful information security requirements: a coping perspective. *Journal of Management Information Systems*, *31*(2), pp.285-318.

Ezzy, D. 2013. *Qualitative analysis*. Routledge.

Fereday, J. and Muir-Cochrane, E. 2006. Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, 5(1):80–92.

GAO (General Accounting Office). 1996. *Content analysis: A methodology for structuring and analyzing written material*. Program Evaluation and Methodology Division, US General Accounting Office.

Gelbstein, E. 2006. *Information security for policy makers: What it means, why it matters, what to do about it?* Retrieved from http://www.unitarny.org/mm/File/Webinars/Unitar%20eg%20presentation%2030_08.pdf [Accessed 14 February 2016].

Gerber, M., Von Solms, R. and Overbeek, P. 2001. Formalizing information security requirements. *Information Management & Computer Security*, 9(1):32–37.

Gerring, J. 2004. What is a case study and what is it good for? *American Political Science Review*, 98(2):341–354

Grant, K., Edgar, D., Sukumar, A. and Meyer, M. 2014. 'Risky business': Perceptions of e-business risk by UK small and medium sized enterprises (SMEs). *International Journal of Information Management*, 34(2):99–122.

Hagen, J., Albrechtsen, E. and Hovden, J. 2008. Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, 16(4):377–397.

Hinchey, M., Bowen, J. and Rouff, C. 2006. *Introduction to formal methods.* NASA Monographs in Systems and Software Engineering, Vol. 1: 25–64.

Hinchey, M.G. and Bowen, J.P., 1996. To formalize or not to formalize. *IEEE Computer*, *29*(4), pp.18-19.

Hofstee, E. 2006. *Constructing a good dissertation: A practical guide to finishing a master's, MBA or PhD on schedule.* Sandton: EPE.

Höne, K. and Eloff, J.H.P., 2002. Information security policy—what do international information security standards say?. *Computers & Security*, *21*(5), pp.402-409.

Hostland, K., Enstad, P., Eilertsen, O. and Boe, G. 2010. *Information security policy best practice document.* UNINETT led working group on security. Retrieved from http://www.book.dislib.info/b1-political/682276-4-produced-uninett-led-working-group-security-no-ufs126-authors-k.php [Accessed 14 June 2016].

Hu, Q., Dinev, T., Hart, P. and Cooke, D., 2012. Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), pp.615-660.

Humaidi, N. and Balakrishnan, V. 2015. Leadership styles and information security compliance behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology*, 5(4):311–318. doi:10.7763/IJIET.2015.V5.522

Jaeger, J. 2013. Human error, not hackers, cause most data breaches. *Compliance Week*, 10(110):56–57.

Johnston, A.C. and Warkentin, M. 2010. Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3): 549–566.

Jurisica, I., Mylopoulos, J. and Yu, E. 1999. Using ontologies for knowledge management: An information systems perspective. In *Proceedings of the Annual Meeting-American Society for Information Science,* Vol. 36. Information Today, 482–496.

Kamp, H. and Uwe, R. 1993. *Introduction to model theoretic semantics of natural language, formal logic and discourse representation theory.* Kluwer Academic.

Knapp, K.J., Morris, R.F. Jr., Marshall, T.E. and Byrd, T.A. 2009. Information security policy: An organizational-level process model. *Computer and Security*, 28:493–508.

Kolkowska, E. and Dhillon, G., 2013. Organizational power and information security rule compliance. *Computers & Security*, *33*, pp.3-11.

Krauss, S.E. 2005. Research paradigms and meaning making: A primer. *The Qualitative Report*, 10(4):758–769.

Leary, M.R., 2016. *Introduction to behavioral research methods*. Pearson.

Leedy, P.D. and Ormrod, J.E. 2005. *Practical research: Planning and design.* Eighth edition. NJ: Pearson.

Lindup, K. 1995. A new model for information security. *Computers & Security*, 14(8):691–695.

Ma, Q., Schmidt, M.B. and Pearson, J.M., 2009. An integrated framework for information security management. *Review of Business*, *30*(1), p.58.

Mackenzie, N. and Knipe, S. 2006. Research dilemmas: Paradigms, methods and methodology. *Issues in Educational Research*, 16(2):193–205.

Marschan-Piekkari, R. and Welch, C. 2011. *Rethinking the case study in international business and management research.* Edward Elgar.

McCune, W., 1994. *Otter 3.0 reference manual and guide (Vol. 9700)*. Argonne, IL: Argonne National Laboratory.

Meyer, B. 1985. On formalism in specifications. *IEEE Software*, 2(1):6–26.

Mouton, J., 2011. *How to succeed in your master's and doctoral studies: A South African* (p. 280). Van Schaik Publishers.

Myers, M.D., 2013. *Qualitative research in business and management*. Sage.

Oates, B.J. 2006. *Researching information systems and computing.* London: Sage.

Orum, A.M., Feagin, J.R. and Sjoberg, G. 2001. *A case for the case study.* The University of North Carolina Press Books.

Palinkas, L.A., Horwitz, S.M., Green, C.A., Wisdom, J.P., Duan, N. and Hoagwood, K. 2015. Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, 42(5): 533–544.

Parkin, S.E., Van Moorsel, A. and Coles, R. 2009. An information security ontology incorporating human-behavioural implications. In *Proceedings of SIN'09.* Pp. 46–55.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. 2014. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, 42(1): 165–176.

Peppard, J. 2007. The conundrum of IT management. *European Journal of Information Systems*, 16:336–345

Princeton University. 2009. *Information Security Policy.* Retrieved from http://www.princeton.edu/infosecpolicy/InfoSecPolicy2009Revision.pdf [Accessed 5 October 2012].

Puhakainen, P. and Siponen, M. 2010. Improving employees’ compliance through information systems security training: An action research study. *MIS Quarterly*, 757–778.

Rees, J., Bandyopadhyay, S. and Spafford, E.H. 2003. A policy framework for information security. *Communications of the ACM*, 46(7):101–106.

Rhee, H.S., Ryu, Y.U. and Kim, C.T. 2012. Unrealistic optimism on information security management. *Computers & Security*, 31(2):221–232.

Riff, D., Lacy, S. and Fico, F., 2014. *Analyzing media messages: Using quantitative content analysis in research*. Routledge.

Ryan P. *Top Tips for Interpersonal Communication*. Boolarong Press; 2014 Oct 21.

Saleh, M.S., Alrabiah, A. and Saad, H.B. 2007. Using ISO 17799; 2005. Information Security Management: A STOPE view with six sigma approach. *International Journal of Network Management*, 17(1):85–97.

Saunders, M., Lewis, P. and Thornhill, A. 2009. *Research methods for business students*. Fifth edition. Harlow: Pearson Education.

Saunders, M., Lewis, P. and Thornhill, A. 2012. *Research methods for business students*. Sixth edition. Harlow: Pearson Education.

Singh, A., Ramakrishnan, C.R., Ramakrishnan, I.V., Stoller, S.D. and Warren, D.S. 2007. Security policy analysis using deductive spreadsheets. In *Proceedings of the 2007 ACM Workshop on Formal Methods in Security Engineering.* ACM, 42–50.

Singh, A.N., Picot, A., Kranz, J., Gupta, M.P. and Ojha, A. 2013. Information security management (ISM) practices: Lessons from select cases from India and Germany. *Global Journal of Flexible Systems Management*, 14(4):225–239.

Siponen, M., Mahmood, M.A. and Pahnila, S. 2009. Technical opinion: Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, 52(12):145–147.

Siponen, M., Mahmood, M.A. and Pahnila, S. 2014. Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2):217–224.

Siponen, M. and Vance, A. 2010. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 487–502.

Sjoberg, G., Williams, N., Vaughan, T.R. and Sjoberg, A.F. 2001. *The case study approach in social research: Basic methodological issues.* The University of North Carolina Press Books.

Sohr, K., Drouineaud, M. and Ahn, G. 2005. Formal specification of role-based security policies for clinical information systems. *ACM Symposium on Applied Computing,* 332–339.

Sommerville, I., 2013. Teaching cloud computing: a software engineering perspective. *Journal of Systems and Software*, *86*(9), pp.2330-2332.

Soomro, Z.A., Shah, M.H. and Ahmed, J. 2016. Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2):215–225.

Stemler, S. 2001. An overview of content analysis. *Practical Assessment, Research & Evaluation*, 7(17):137–146.

Swanborn, P. 2010. *Case study research: What, why and how?* London: Sage.

Thomson, K.L., Von Solms, R. and Louw, L. 2006. Cultivating an organizational information security culture. *Computer Fraud & Security*, 2006(10):7–11.

Trček, D., Trobec, R., Pavešić, N. and Tasič, J.F. 2007. Information systems security and human behaviour. *Behaviour & Information Technology*, 26(2):113–118.

Vance, A., Lowry, P.B. and Eggett, D. 2013. Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, 29(4):263–290.

Van Niekerk, J.F. and Von Solms, R., 2010. Information security culture: A management perspective. *Computers & Security*, *29*(4), pp.476-486.

Von Solms, B. and Von Solms, R. 2004. The ten deadly sins of information security management. *Computers & Security*, 23:371–376.

Whitman, M.E. 2004. In defense of the realm: Understanding the threats to information security. *International Journal of Information Management*, 24(1):43–57.

Whitman, M.E. and Mattord, H.J. 2012. *Principles of information security.* Boston, MA: Cengage Learning.

Williams, P.A.H. 2008. In a ‘trusting’ environment, everyone is responsible for information security. *Information Security Technical Report*, 13(4):207–215.

Woodhouse, S., 2007, October. Information security: End user behavior and corporate culture. In *Computer and Information Technology, 2007. CIT 2007. 7th IEEE International Conference on* (pp. 767-774). IEEE.

Wynn, D. Jr. and Williams, C.K. 2012. Principles for conducting critical realist case study research in information systems*. MIS Quarterly*, 36(3):787–810.

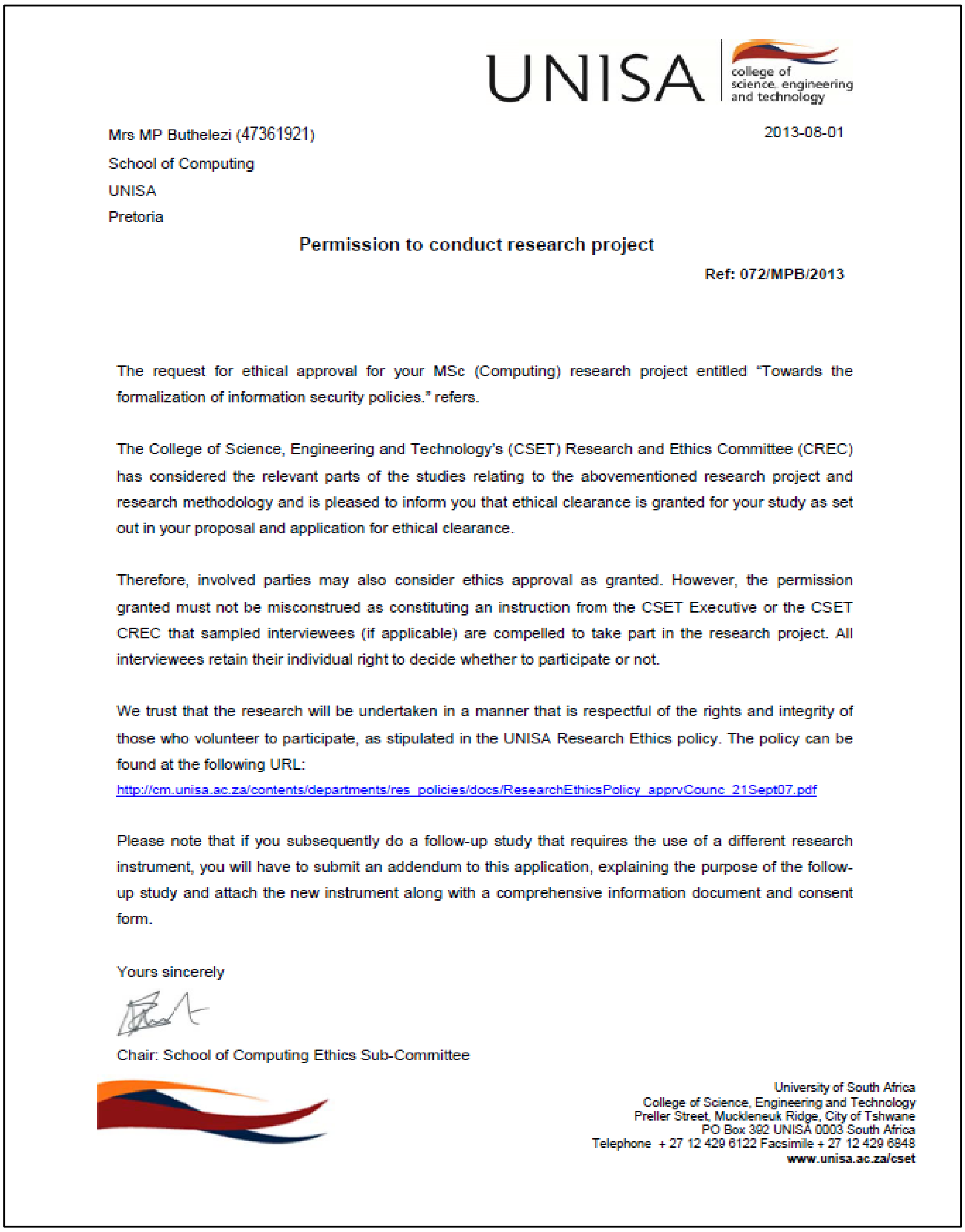
Xifra, J. and Girona, R. 2012. Frank Capra's Why We Fight and film documentary discourse in public relations. *Public Relations Review*, 38(1):40–45.

Yarowsky, D. 1994. Decision lists for lexical ambiguity resolution: Application to accent restoration in Spanish and French. In *Proceedings of the 32nd annual meeting on Association for Computational Linguistics*. Association for Computational Linguistics, 88–95.

Yin, R.K. 2009. *Case study research: Design and methods.* Fourth edition. London: Sage.

Appendices

Appendix A: Ethical clearance certificate



UNISA college of science, engineering and technology

Mrs MP Buthelezi (47361921)
School of Computing
UNISA
Pretoria

2013-08-01

Permission to conduct research project

Ref: 072/MPB/2013

The request for ethical approval for your MSc (Computing) research project entitled "Towards the formalization of information security policies." refers.

The College of Science, Engineering and Technology's (CSET) Research and Ethics Committee (CREC) has considered the relevant parts of the studies relating to the abovementioned research project and research methodology and is pleased to inform you that ethical clearance is granted for your study as set out in your proposal and application for ethical clearance.

Therefore, involved parties may also consider ethics approval as granted. However, the permission granted must not be misconstrued as constituting an instruction from the CSET Executive or the CSET CREC that sampled interviewees (if applicable) are compelled to take part in the research project. All interviewees retain their individual right to decide whether to participate or not.

We trust that the research will be undertaken in a manner that is respectful of the rights and integrity of those who volunteer to participate, as stipulated in the UNISA Research Ethics policy. The policy can be found at the following URL:
http://cm.unisa.ac.za/contents/departments/res_policies/docs/ResearchEthicsPolicy_apprvCounc_21Sept07.pdf

Please note that if you subsequently do a follow-up study that requires the use of a different research instrument, you will have to submit an addendum to this application, explaining the purpose of the follow-up study and attach the new instrument along with a comprehensive information document and consent form.

Yours sincerely

Chair: School of Computing Ethics Sub-Committee

University of South Africa
College of Science, Engineering and Technology
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone + 27 12 429 6122 Facsimile + 27 12 429 6848
www.unisa.ac.za/cset