UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

Case Study: An Evaluation of the comprehensibility of information security policies in a South African bank

By

Riyadh Sayed Razack

200202020

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

School of Management, Information Technology and Governance

Discipline of Information Systems and Technology

College of Law and Management Studies

Supervisor

Professor M Maharaj

2023

DECLARATION

I, Riyadh Sayed Razack declare that

(i) The research reported in this dissertation/thesis, except where otherwise indicated, is my original research.

(ii) This dissertation/thesis has not been submitted for any degree or examination at any other university.

(iii) This dissertation/thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

(iv) This dissertation/thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers.

Where other written sources have been quoted, then:

a) Their words have been re-written but the general information attributed to them has been referenced;

b) Where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

(v) Where I have reproduced a publication of which I am author, co-author or editor, I have indicated in detail which part of the publication was actually written by myself alone and have fully referenced such publications.

(vi) This dissertation/thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the dissertation/thesis and in the References sections.

Signed  Date: 19 June 2023

ACKNOWLEDGEMENTS

All praises are first due to the Almighty creator, knower of all, oft forgiving and most merciful.

My most sincere thanks to my mother Tasneem and father Sayed who have sacrificed much for me and my education, instilling in me a drive to better myself and the importance of knowledge in not only alleviating poverty and strife, but making good life choices as well. Thank you both for your support and guidance throughout my life, teaching me perseverance and patience.

My profound gratitude goes to my Supervisor, Professor Manoj Maharaj for his support, guidance, patience, and assistance in completing this research. The direction and alternative methods of problem solving have been novel and appreciated as I have not been an easy student to supervise, and this research exercise was paused and resumed a number of times.

To my wife Zainab for her patience and understanding.

ABSTRACT

Information security policy and its resultant implementation is seen as pivotal in organisations that want to protect their information both internally and externally. Employees are relied heavily upon to read and understand and therefore comply with the information security policy including all its principles. The study has used readability and comprehension tests to assess the policy to analyse what the minimum required reading level is, how much abbreviations and jargon are contained therein. Employees were surveyed to understand the implications of security policy on them, the study utilised interviews of staff and asked questions pertaining to awareness, ideal ways to eradicate jargon and technical terms as well as views around security policy implementation. Ultimately directing implications around improvements to be made, but not limited to the removal of jargon and technical terms. Further to this, recommendations are detailed for policy writers and implementors, as well as critical success factors for ISMS managers and security specialists who are tasked with crafting policy, embedding this through the organisation and ensuring staff comply and adhere to organisational information security strategy. A conceptual multi-dimensional framework to coordinate the significant outcomes identified in the study is also developed to enable robust information security design, and monitoring. Within the context of the study a number of important and noteworthy outcomes have been established. Any conceptual framework must provide a dimension to remediate the readability challenges. The other established outcome pertains to awareness and socialisation/training pertaining to policies, where respondents did not believe awareness of information security policies were adequate and accessibility was viewed as problematic, this was confirmed by the interviews where most staff did not know where to locate information security policy/ies. Respondents did not feel included in the development of policy and accompanying improvement mechanisms and consequently any conceptual framework which does not incorporate users is inherently flawed.

Keywords: Critical Discourse Analysis, Information Security, ISMS, Readability, ISO27001

LIST OF ABBREVIATIONS

Number	Abbreviation	Full Name
1.	ANOVA	Analysis of variance
2.	ANSI	American National Standards Institute
3.	CDA	Critical Discourse Analysis
4.	COBIT	Control Objectives for IT
5.	COSO	Committee of Sponsoring Organisations
6.	IEC	International Electrotechnical Commission
7.	IP	Internet Protocol
8.	ISMS	Information Security Management Systems
9.	ISO 27001	International Organisation for Standardization – Information Technology – Security Techniques – Information Security Management Systems
10.	ITIL	Information Technology Library
11.	JTC	Joint Technology Committee
12.	PIRLS	Progress in International Reading Literacy
13.	POPIA	Protection of Personal Information Act
14.	RANDBETWEEN	Formula in MS Excel for Randomizing data
15.	SMOG	Simple measure of gobbledygook
16.	SWOT	Strength, Weaknesses, Opportunities and Threats
17.	T-Test	Single sample t-test

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

Introduction

1.1 Information Security Policies and Organisational Context

South Africa remains one of the most socially and economically unequal countries in the world (World Bank, 2022). These inequalities typically emanate from historic financial and educational segregation perpetuated over decades and attributed to the apartheid regime (Christie, 2006). Researchers argue that even though the political machine responsible for the exclusion of some to the benefit of others has fallen, the practice of exclusion is still rife but decidedly more overt (Wambugu, 2006). It is this exclusion either intentionally or unintentionally that creates stratification in society and further widens the divide between those with easy access to resources and education and those without such access.

Globalization has created possibilities for collaboration between nations and individuals on an unprecedented level, in both private and public sectors, enabling the sharing of ideas across continents to the benefit of many and has served to reduce poverty (Shin, 2009). But, in many instances, in South Africa, abject poverty and lack of education persists. This lack of education is seen as a limiting factor to the uptake of knowledge and to the advancement of communities and people and has become normalised in society to a large degree (Walker, 2007).

These inequalities are manifest in societies the world over including in developed nations (Wood, 1998) and are therefore consequently reflected as issues within the workplace as well. Inequalities and their relation to information security and its practice and communication are important as the Fourth industrial revolution and digitisation of the economy become important factors (Moavenzadeh, 2015). Therefore, as technology evolves and becomes more interwoven with daily life, how do information security policymakers and governance managers then align to facilitate management and monitoring into the future?

With information technology use already ubiquitous (Hoehe and Thibaut, 2020), organisations worldwide seek to govern and control the use of information assets and

associated technology through various policies and procedures. This has resulted in several cooperatives, government institutions and private sector organisations as well as academics creating, asserting, and adopting frameworks, operating standards as well as significant nascent thought leadership in the domain. As such, a global community of experts, some with financial interests in the matter, scramble to advance adoption of what is widely accepted as industry best practice. This has taken the form of policies, procedures, certifications, and qualifications for security practitioners.

As all material composed within an organisational context comprises largely of written materials, comprehension of reading materials is important to ensure readers can access information adequately, but also to ensure there is proper and effective communication of key messages, rules, law, and strategy. Comprehension as it pertains to written materials has been widely analysed. According to Woolley (2011), "It is a two-way process that integrates information from the text-based models with information from prior knowledge using inferential processing." This ultimately creates a basis of understanding in the reader, sometimes impacted specifically where internal or external limitations to reading comprehension may be possible.

Internal limitations centre around biological (such as dyslexia, colour-blindness) factors, as well as cognitive and behavioural limitations. External limitations on the other hand pertain to inadequacy of the materials, language, tone, and assumptions made upon the underlying reading capability of the reader. For the purposes of this study, focus has been given to external limitations which may impede the overall discourse centred around information security policies and procedures and how they are impacted by comprehension.

1.2 Background and Context for Study

Within organisations, adoption of information security policies and procedures is considered routine and fundamental to its overall security programme. Mandatory training and annual attestations mean that all staff and associated parties including vendors are expected to be familiarised and accountable for ensuring adherence to these policies and procedures. As information technology advances though, it has become more challenging to ensure that these policies remain relevant and intelligible in an ever changing and rapidly advancing technological context.

Expectedly, literacy and readability (the ease of reading and understanding a policy) are very important factors that would influence an organisation's overall security programme or any training and awareness programme for that matter, since the policies are the initial discourse available to staff. Simply put, if staff cannot read and understand policies and procedures, then they cannot be expected to internalise and implement adequate information security best practice personally or in an organisational context. This impediment then nullifies any security programme or awareness initiative and may serve to undermine the overall information security strategy of an organisation.

From a South African point of view, a Progress in International Reading Literacy (PIRLS) in 2016 study, placed South African children last out of 50 countries and found that the scores had not improved since 2011 (Howie et al., 2016) and a new study conducted in 2019, found that not much improvement had been made between 2016 and 2019 (van der Berg and Gustafsson, 2019) where it was estimated that 78% of learners in South Africa could not read for comprehension by the conclusion of Grade 4. This number has since deteriorated in 2021 with 81% of Grade 4s unable to read for meaning (Reynolds et al., 2021). This therefore evidences a decline in the reading levels as per the studies conducted since 2011. Many organisations now consider a tertiary qualification as a minimum hiring requirement to ensure minimum education levels and literacy, even though research has proven that even at university undergraduate levels, reading for comprehension remains problematic and students encounter significant challenges (Wilfred Molotja, 2020). However, this requirement is not retrospectively applied and there are staff within organisations who were employed before the minimum tertiary requirement was introduced with varying levels of literacy. Noteworthy though, is that while literacy alone is not a measure of internalisation of organisational content, comprehension however, is (Davis et al., 2006).

Ultimately though, an information security programme is only as strong as the weakest link, and in almost every breach or large-scale hack, it is the "people" aspect of the technology triangle (People, process, technology) that is considered weak and prone to attack and consequently targeted (Bulgurcu, Cavusoglu and Benbasat, 2010).

If staff cannot understand and interpret an information security policy or procedure, then these same staff cannot, and will not act according to its intent. Therefore, staff inadvertently expose data, details and sometimes trade secrets without even realising they are doing so. This usually occurs to the detriment of the organisation's responsibilities to its clients and customers, but directly to the detriment of staff implicated in non-adherence especially where dismissal may be a likely outcome as a consequence. Basically, the organisational stance taken is that staff have read, understood, and attested to comprehension of the information security policies and procedures and are expected to strictly adhere to it regardless of changing circumstances, differing levels of comprehension and education as well as vastly varying access to organisational data and confidential information, even though comprehension in this context is not verified. Organisations assume staff who have read information security policies, understand them as well.

Organisations have realised that simply training only senior staff where information security is concerned, is ignoring the fact that most if not all staff during duties, are privy to data and therefore all information security programmes must target all staff alike and, in some cases, identify critical or high impact/risk staff for specialised programmes (Khando et al., 2021).

1.3 Problem Statement

The ongoing challenge organisations face is ensuring that all IT policies and procedures are written clearly and are readable by all within the organisation who are exposed to the information assets. Not only this, but in instances where breaches and data loss occur, an employee or impacted person may be subjected to disciplinary and criminal procedures to protect the organisation against any liability, financial or reputational that may result. In some cases, these incidents are public knowledge and publicised as well and staff impunity is not tolerated well from a reputational perspective externally. One of the concerns identified with such procedures is that an employee may not have fully understood or comprehended the intent of an information security policy and consequently may have acted in contravention of said policy/procedure, purely due to ignorance based on impaired comprehension capability. There currently does not exist any confirmation of comprehension since staff only certify that they have read the policy.

Having read a document is not an indication of having internalised the content and its direct and indirect implications.

In dismissal cases, an employee may contend that ignorance with respect to a policy is a valid reason to avoid dismissal or criminal proceedings. Essentially, the information security documents need to convey the core message and intent in a manner that can be understood readily by its reader regardless of literacy levels. The policies are written with an implicit understanding that the reader is capable of reading at a certain minimum level. However, this is not immediately obvious, as organisations employ people of varying degrees of competence (also language competence), many of whom have access to the company's information assets.

Not only this, in cases of dismissal, an organisation is required to indicate in detail the lengths it has gone to deliver the information security intent to the employee in a simple, understandable, and consistent manner from a legal standpoint and in order not to unfairly dismiss an employee contending ignorance of a policy and its implications. Further to this, it is imperative that policies acknowledge and accommodate the changing technology landscape and the body of knowledge that is created consequently.

To achieve this, information security policies categorise data across the organisation according to confidentiality classifications. The policies themselves seek to define and govern the information security domain, access levels, standards to be applied and protection mechanisms like encryption are therefore detailed and ultimately define the boundaries of data use and protection. These mechanisms described in the policy create the underlying fabric protecting internal and often confidential data from the external environment.

With respect to the implications to information technology, it is important to note that it is accepted often by industry experts and businesses that an undue focus on technology with a consequential lack of focus in people and process is perilous (Fielding, 2020). Therefore, the logical outcome must be that for people/staff in an organisation to understand and practice proper information security principles, they must first understand those principles in a meaningful and actionable way.

There are several characteristics that may influence readability and comprehension of information security policies and procedures such as language, acronyms and jargon, tone, ambiguity and simplicity in the underlying intent without introducing complexity. These factors are examined in detail within the context of this study. The study is conducted at a large Financial Services organisation in South Africa. The researcher is permanently employed within the organisation as a Risk Specialist.

1.4 Information Security Management Systems (ISMS)

While several frameworks and rubrics exist within the information security domain of IT with a specific focus on organisational preparedness and security counter-measures, none of the frameworks concentrate on ensuring the ease of use and consumption of policies, procedures, and training material applicable in the aforementioned context.

The most widely accepted methodology or framework for security currently is the Information Security Management System or ISMS as it is commonly known (Shojaie, Federrath and Saberi, 2015). The ISMS was created as a practical instrument for the implementation and institutionalization of ISO 27001:2013 (International Organisation for Standardization – Information Technology – Security Techniques – Information Security Management Systems). This internationally accepted global standard defines all requirements for creating, implementing, maintaining as well as improving an organizational information security management system. Further, the standard also dictates the requirements for an assessment and treatment of information security risks in an organization. Importantly, the standard is designed to be generic, and agnostic of technology solutions to information security risks and applicable to all organizations, regardless of field, size, or complexity (ISO, n.d.). It is for this reason it is considered the most renowned standard for information security implementations the world over (Culot et al., 2021).

In the wider context of why organisations choose a specific standard or framework, it is important to understand that while there are several frameworks and standards, for security as a practice, large organisations do not select frameworks arbitrarily since they are often accompanied with significant compliance overhead and possible certification especially in the case of ISO 27001. The ISMS framework is a well-established and widely adopted framework for managing information security and provides a

comprehensive approach to managing information security by addressing assets, threats, and vulnerabilities (Susanto, et al., 2020). Additionally, to ensure efficient and adequate information security management, the use of an ISMS has been identified as a critical success factor (Tu, et al., 2014).

The International Standards Organisation itself conducts an annual survey of certifications and sites across all industry sectors with results announced the following year, therefore in arrears. Their 2021 study, published in 2022 states that adoption rates are increasing and in South Africa, 106 certificates were issued, up from 78 in the previous period (ISO Survey Certifications). Certification entails full implementation of ISO27001 including accompanying standards and policies that support the framework as well as auditing and remediation usually conducted by an external organisation who certify compliance.

In South Africa, there are governmental policies that advocate for the use of international standards, such as ISO 27001, for information security management. To this end, the South African government has developed a National Cybersecurity Policy Framework (NCPF) to address cybersecurity issues and promote a secure and resilient cyberspace.

While the NCPF does not explicitly mention ISO 27001, it does emphasize the importance of adopting internationally recognized standards and best practices for information security (Bote, 2019). ISO 27001 is a widely accepted standard for information security management systems (ISMS) and is often used as a benchmark for organizations seeking to improve their cybersecurity posture.

In addition to the NCPF, the Protection of Personal Information Act (POPIA) is another piece of legislation in South Africa that deals with information security, specifically personal data. POPIA requires organizations to implement appropriate security measures to protect personal information. Although it does not specifically mention ISO 27001, organizations can use the standard as a guideline to help them comply with POPIA's requirements (Moraka and Singh, 2023).

It is therefore no surprise, that this industry standard is widely applied in South Africa across organisations that do not certify with the ISO but adopt and implement the

standard, albeit, often in limited capacity since it is viewed as the minimum standard. This is further institutionalized with assurance providers and auditors all assessing the implementation of IS27001:2013 by assessing the effectiveness of the ISMS and its principles at organisations, typically on an ongoing basis.

As ISMS implementations are therefore widespread internationally including in the South African context and advocated by government itself, it is possible to establish the acceptance and implementation of the ISMS at the study site as not only in keeping with international best practice across industries and sectors but mandated by government directly as well.

The question that then requires answering, is that if ISMS implementations are widespread, why then do breaches and incidents still persist (Zaini and Masresk, 2013)?

One study conducted by Almutairi and Alshammari (2019) examined the readability and comprehensibility of the ISMS Information Security Framework. The study found that the language used in the framework was complex and difficult to understand for many users. The authors recommended that the framework be revised to use simpler language and to provide more examples and explanations to aid comprehension.

Another study by Alshammari and Almutairi in 2020 examined the use of visual aids in the ISMS Information Security Framework. The study found that the use of visual aids, such as diagrams and flowcharts, improved comprehension and understanding of the framework for many users. The authors recommended that the framework be revised to include more visual aids to aid comprehension.

A third study by Alshammari and Almutairi (2021) examined the use of plain language in the ISMS Information Security Framework. The study found that the use of plain language, which is language that is clear and easy to understand, improved comprehension and understanding of the framework for many users. The authors recommended that the framework be revised to use plain language to aid comprehension.

Overall, these studies suggest that the language used in the ISMS policies can be problematic for some users. To improve comprehension and understanding of the

framework, it may be necessary to revise the language used, provide more examples and explanations, and include more visual aids. By doing so, organisations can ensure that the framework is effectively implemented and that information security measures are properly implemented and maintained.

Moreover, a study published in 2021 further investigated the challenges faced by organisations in implementing ISO27001, via the use of an ISMS policy. The study identified communication and language barriers as significant challenges, particularly when translating the standard's requirements into actionable tasks. The authors suggest that organisations should invest in training and awareness programs to improve comprehension and readability of the ISMS requirements which would allow for better outcomes (Culot et al., 2021). Additionally, it is important to realise that often, the only documents or information available to employees concerning what constitutes good information security is contained in the very documents that are inherently flawed to begin with. They are without any clarification and do not allow opportunities to ask questions and over time become the codex with which information security is practiced at the organisation (Flowerday and Tuyikeze, 2016). This means that a lack of clear definitions and understanding of information security creates a culture which can lead to ineffective ISMS implementations (Mahfuth et al., 2017).

In terms of compliance however, assuming communication efforts (posters, emails, awareness training) are adequate, the readability of information security policies are identified as a significant factor impacting overall information security culture (Alzahrani et al., 2018) highlighting clear, concise language as a critical success factor.

The next problem is whether or not research on readability of information security policies and implementation flaws of ISO 27001 via an ISMS is addressed by the ISO Organisation at all since research on the topic indicates issues.

While the 27001:2013 standard has a section specifically for policies, the stipulation/or minimum requirement specified that is relevant to policy is limited to:

- Being available as documented information;
- Communicated within the organization; and
- Being available to interested parties, as appropriate.

As is evident therefore, a critical failing is that there is no emphasis on the readability or ease of use of the ISMS policies and procedures. Not only this, but there is also no immediately identifiable mechanism to assess this vulnerability which can have a significant impact on a policies resultant implementation as has been established by existing research on the topic.

Policy implementation research shows that even when concerted efforts are made to implement policies properly, failures continue (Anderson, 2001). The consequent assertion made from this vantage point is that "viewing implementation failure exclusively as a result of poor policy clarity deliberately attempts to ignore the complexity of the human sense-making processes consequential to implementation" (Honig, 2006). It therefore stands to reason that poor security policy documentation and procedures will result in poor security programme implementation ultimately negatively affecting the outcomes for a successful security campaign (Eybers and Mvundla, 2022).

The question that is then created is one pertaining to metrics for analysis, or primarily, research methods to be used to dissect information security documents/policies then analysed to inform a result around adequacy from a language, tone, jargon and general conciseness perspective since the analysis mechanism must have scientific basis and satisfy empirical scrutiny. This includes matters of repeatability, reliability, sound basis and wide acceptance by subject matter experts.

While there are no methods specific to information security policies, a widely accepted method for analysing any written communication must be used.

1.5 Critical Discourse Analysis (CDA)

Critical Discourse Analysis (CDA), is an interdisciplinary approach to the study of discourse that views language as a form of social practice and discourse on a subject. CDA combines critique of discourse and explanations of how the existing information contributes to the social reality, as a basis for action to change.

By examining the readability of texts within CDA, researchers can analyse and understand potential strategies employed by dominant discourses to maintain their influence and exclude certain groups or perspectives. CDA allows for an examination of linguistic accessibility, the use of technical jargon, or complex sentence structures that may inadvertently or intentionally exclude marginalized communities from fully engaging with the text. It provides a quantitative measure to complement qualitative analyses, enriching an understanding of how power operates through language in different discourse domains (Fairclough, 2013).

In the context of information security, CDA can prove useful as an essential methodology to analyse written documents, and within the framing of this study, it can be used to analyse information security policy.

Within the framework of Critical Discourse Analysis, researchers employ various methods to analyse text and documents and reveal underlying power structures and ideologies as well as to identify design flaws. One method that is used is Fry's Readability Instrument. Developed by Rudolph Fry in 1968, this instrument assesses the readability or linguistic complexity of a text based on sentence length and word familiarity (Fry, 1968). By applying Fry's Readability Instrument to texts analysed through a critical lens, researchers can gain insights into how language choices may shape power relations, reinforce social hierarchies, or create barriers to understanding.

Fry’s Readability Instrument is a proven scientific rubric and its resultant graph which categorise a documents’ ease of being read and understood according to varying levels of literacy (Fry, 1989; Courtis, 1995) is easy to use. Within CDA, it is not prudent to use a sole instrument since no method is established as more prominent than another, and researchers typically combine the use of multiple instruments to strengthen the reliability of testing and ensure the validity of results since each instrument has strengths and weaknesses (Wodak and Meyer, 2016).

Another supporting model used to analyse readability of documents is the Cloze test or Cloze deletion test (Taylor, 1953). Using this method, every fifth word of the first 250

words of a document is replaced with blanks and study subjects are asked to guess-replace them contextually.

Finally, the SMOG (Simple Measure of Gobbledygook) is another readability formula under the CDA domain developed in 1969 by Harry McLaughlin to calculate the difficulty of a text based purely on the number of polysyllabic words contained therein (McLaughlin, 1969).

The above methods within the broader auspices of CDA are further expanded on and analysed for their potential application in this research as they apply to the information security policies and procedures at the financial services organisation given the established problems identified with policies and readability.

1.6 Research Questions and Research Aims

Policy implementation challenges are numerous ordinarily but more so where information security and technology intersect (Alotaibi, Furnell and Clarke, 2016). Staff in an organisation must keep abreast of technological advancements that are applicable to their daily duties and conform to best practice as adopted by the organisation. Non-conformance carries penalties and repercussions far wider than the individual and can result in significant losses reputationally or financially for the organisation involved. Therefore, staff must be able to comprehend information security policies and procedures and always act in accordance with them.

Consequently, the following key research questions are identified within the study:

1.6.1 Research Questions

1. Are the organisations' information security policies problematic within the context of critical discourse analysis and using the accompanying scientific rubrics?
2. What are the appropriate mechanisms to be used to convey the organisational intent as it pertains to information security?
3. Are dissemination and communication methods adequate?
4. Are there potential pitfalls associated with the current awareness programme?

5. Is there a framework/set of guidelines and constructs that can assist policy implementors and subject matter experts to create a robust ISMS policy?

Answering these questions will essentially entail analysing the policy at the organisation using the instruments and identifying additional sources of information to enrich the overall outcome and validate any findings in terms of convergence or variance.

Consequently, the key research aims as well as outcomes for this study include:

1.6.2 Research Aims

- Assessing the comprehensibility and readability of organisational information technology security policies using Fry's readability model, Cloze deletion test as well as the SMOG test. Additionally, the inclusion of critical discourse analysis to further dissect the intent being communicated will inform the outcome of whether the use of jargon and specific language detracts from, or conversely supports the communication of intent of said IT security policy.
- To conduct critical discourse analysis to understand if socio-political biases pervade the policies and procedures to the point of inclusion of some staff at the inadvertent exclusion of others including Identifying the appropriate mechanisms to ensure that the intent of an information technology policy is conveyed and what methods are to be used. If policy comprehension itself is problematic and not effective, then what other methods can be used, and will that result in improved information security policy implementation by itself, and if not, what other characteristics are relevant and important to consider and augment within the organisation.
- The development of a conceptual or theoretical framework that will aid organisations in developing information security policies and procedures that are easily understood by all staff within the organisation to successfully embed and entrench the security programmes required to secure the organisation from security risk resulting in a more robust ISMS implementation. This may include the automatic onboarding of documents through "scanning" or filtering tools to identify whether the text s contains too much jargon and is unreadable by the intended audience.

1.7 Research Rationale

From a research point of view, Critical Discourse Analysis (CDA) has been expansively used in linguistic practice but more recently, with globalisation and organisations expanding across nation borders seen prominence in social sciences, anthropology, and politics (Lupton, 2010). Studies have analysed readability and comprehension in schools, general society as well as the medical sector (Snyman, 2004).

While based within the social sciences, CDA however has been used to analyse discourse, i.e. policies within the domain of information security (Knudsen and Löfgren, 2018) and further research is analysed within existing literature regarding the use of, applicability and limitations of CDA use in information security.

The outcome is that ultimately, this research will result in the creation of a conceptual and theoretical framework or measurement characteristics that can be universally applied to Information Security policies and procedures within the organisation.

1.8 Significance of the Study

The critical outcome of the research is to assess and measure the organisations' key/ primary information security policy from a readability and comprehensibility point of view against the background of an ISMS programme and implementation. Further, the research instruments used (surveys and interviews) further aim to add a personal dimension from staff perspectives which may not necessarily be expressed through the clinical discourse methods employed such as the Fry's readability analysis, Cloze test, or the SMOG test.

Therefore, a qualitative and quantitative approach, or mixed methods approach is used to enrich and prove the research outcomes. By analysing the policies through the critical discourse methods and comparing the results against views expressed by staff via the interviews, the study will produce a distinct measure of readability of the policies, expressing understanding of intent and specifically within the context of CDA, valid measures around security discourse within the organisation.

This research is not only important as it pertains to information security policies and their implementation, but broadly relate to technology use and adoption within any organisation that must be governed and guided through the use of policies and written discourse.

Wider than this, the study has implications for policy creation across the organisation and potential learnings that can be applied for all discourse situations.

1.9 Structure of the Study

Chapter 1 introduces the overall context for the study and operating environment as it relates to industry best practice, policy use, information security posture and awareness programmes. This chapter includes indicating the research problem itself, objectives, aims, rational, significance of the study and expected outcomes.

Chapter 2 considers existing literature on the subject of readability as it pertains to critical discourse analysis as well as an analysis of the discourse rubrics that are used to assess readability and its implications for information Security policy implementation in an organization as well as the shortcomings of the mechanisms. Further, the ISO Standard pertaining to Information Security programmes is introduced and its implications for an ISMS implementation is analysed. Finally, the limitations and operating parameters used in previous studies on the subject of information security policy adoption and awareness programmes are established from previous studies on the matter. All relevant models are critically reviewed in terms of their efficacy and reliability.

Chapter 3 details the methods and mechanisms utilized for the study, including detailing the research hypothesis, strategy, design, research sites, population, and sample methods. The reason for the use of qualitative methods as well as surveys and finally the interviews conducted and their implications and relevance to the study. Any ethical implications, limitations in the study philosophy and constructs are also detailed in this chapter as well as any omissions or scope exclusions or limiting factors.

Chapter 4 presents the outcomes from analysing the policies via the clinical methods outlined and their results. Where possible graphical representation is used to present the

underlying data outcomes. Additionally, the themes emanating from interview responses and any statistical data outliers are also explained and analysed in this chapter. The intersection between results in the clinical methods and the interviews are then analysed and juxtaposed to compose on overall view and resultant posture regarding the organisations' Information Security policies. Statistical analysis of the surveys is also performed, and the outcomes analysed and discussed in this chapter. This chapter also details the formulation and discussion of the theoretical framework that can be implemented to ensure IT Security policies are designed to address comprehensibility and usability shortcomings including ensuring the avoidance of jargons and acronyms while still communicating IT security policy intent clearly.

Chapter 5 is a summative view of the comprehensibility of the Information Security policy within the organization. This chapter also concludes whether the research intent was met and if there are any pertinent outcomes or questions that emanate that necessitate further analysis or study not covered in this Case Study. All recommendations are presented in this chapter and research failings and limitations mentioned as well.

1.10 Conclusion

This chapter has introduced Critical Discourse analysis and its relevance to Information Security policy implementation, adoption, and awareness. Moreover, the chapter introduces the use of ISMS across the industry including its limitations where policy guidance is concerned. In addition, the research questions, aims, objectives and rational have been detailed as well as the research context and background and macro factors influencing the relevance of the study.

The following chapter introduces existing research on the subject, the models used to assess and monitor comprehensibility as they pertain to linguistics and its relevance to information Security within the domain of CDA. ISMS as a framework is introduced and analysed from an effectiveness and applicability point of view as well as the application of the models to information security research. A critical analysis of existing and underlying factors affecting previous studies adjacent to the subject matter is also presented and discussed.

CHAPTER 2

Literature Review

2.1 Introduction

The weakest link in information security systems remains that of employees (Bulgurcu, Cavusoglu and Benbasat, 2010). Inadvertently exposing corporate information externally through social media, reusing and writing down passwords, clicking and responding on phishing emails as well as several other foibles, ultimately resulting in a weakened security posture (Colwill, 2009). Therefore, organisations that realize this core failing, cater for it and formulate policies and procedures that are effective in communicating both desirable and undesirable behaviour in relation to information technology, will succeed in their efforts (Bulgurcu, Cavusoglu and Benbasat, 2010).

Creating, formalising, and communicating effective and all-encompassing information security policies thus become paramount in managing the challenges faced within the information security domain. While many organisations worldwide have drafted policies and procedures with specific information security content based on well tested and popular international standards, breaches are still commonplace with increasing complexity and associated losses (up 12.7% from 2020) for the businesses that incur them (2022 Cost of Data Breach Study: Impact of Business Continuity Management, 2022). Consequently, the question that arises is that if subject matter experts, industry experts and financial sector regulators contribute toward the information security policy science as a practice, then why do IT security breaches still persist? The conclusion that can be drawn from this, is that communication mechanisms, language, and other mechanisms that organisations use to convey this message are inherently problematic. Therefore, it can be inferred that the above contribute to a failure to understand threats and respond within a cyber security context, but also to begin to take offensive action against threat actors and conspiring countries (Carr, 2012) as a consequence.

The processes used to create these documents, communicate them, as well as implement them within organisations is important. However, even the best planned and executed policy formulation processes still depends upon the end-user understanding them consistently and easily.

Understanding documents can be dissected into two identifiable domains, that of readability which pertains to the document itself and its various characteristics as well as that of comprehensibility, which is the ability of the document to be understood (Graesser et al., 1994).

2.2 Comprehension

According to Elleman and Oslund (2019), reading comprehension is one of the most complex cognitive activities that humans engage in, therefore making it difficult to teach, measure and study since comprehension can be heavily influenced by reading ability, recollection, inferential ability as well as vocabulary and prior knowledge (Perfetti et al., 2005).

To consider comprehension and its implications in policy design and implementation, it is essential that it is analysed in the context of how people understand and respond to the rules and regulations that govern their behaviour and rights, and within the context of this study, their responsibilities within the organisation as it pertains to information security. Policies are often written in complex, technical language and include jargon and abbreviations, which can be difficult for ordinary people to understand. Within the organisational context, this can lead to confusion, misunderstandings, policy violations and even litigations and fines. It is therefore important to make the documents more readable, accessible, and transparent to the reader, thereby scientifically improving comprehension.

Unpacking the causes and outcomes from policy failures has been studied specifically as it pertains to what happens between policy formulation and policy implementation and how comprehension is one of the more significant factors (Hudson et al., 2019) including reliable frameworks and sound interpretation of laws, rules, and regulations.

Research has centred on the assumption that policies do not succeed or fail on their own, but instead potentially fail as a consequence of the complex and chaotic systems in which they operate. The outcome ultimately proposed by researchers on comprehension failure suggests that policy failure can be avoided by strengthening and supporting the policy

process especially at the developmental and implementation stages (Cairney, 2015). This phase of policy implementation directly correlates to and has the largest impact on comprehension since early indicators of policy uptake, and thereby its intent, and long-term outcomes become evident, and can be rapidly amended via adequate feedback mechanisms (Pashler, 2007).

Critical failure characteristics that are identifiable include a lack of clarity, incoherence, legitimacy as well as ownership and ultimately the feedback loop for the above (Hudson et al., 2019). Therefore, we can understand from research on comprehension that failures may be manifold and are often difficult to distinguish from one another given the close interdependence of characteristics on each other ultimately all affecting comprehension.

To analyse the readers comprehension independent of the operating environment is inadequate since instances where the implementation environment is complex such as the organisational context, uncertainty, ambiguity and interdependence on other policy sets, documents, and frameworks (as is the case with Information Security policies) serve to complicate overall comprehension and create problems with identifying one single causal factor. From the readers perspective, this creates a policy context where documents reference other documents and policies and must be read together. Further, since frameworks are meant to be the basis on which policies are created, instances where frameworks are at odds with each other and offer conflicting solutions to similar problems, the creation of further comprehension impediments is noted. Ultimately, this creates a situation where measuring comprehension is made difficult and imprecise (Cain, 2006).

In order to analyse comprehension more deeply researchers have studied the complex and multi-faceted approaches of automaticity (or the ability to read naturally) which has the benefit of allowing readers to devote more cognitive attention to comprehension (versus the converse of trying to understand each part of a sentence in a document or text) (Duke, 2021).

Therefore, we can understand that comprehension is affected by characteristics wider than the content of the document or text and that there appears to be significant correlation between reading comprehension and the strategy employed to improve it (Yuanke et al.,

2021). These strategies are influenced by cognitive development which appears stronger in more experienced readers as opposed to their younger counterparts given the accumulation of potentially more substantial prior knowledge (although newer readers can have more prior knowledge of a given subject matter versus their contemporaries) which then means that prior knowledge factors significantly into comprehension. Qualitative methods are often used by researchers to analyse this domain construct and its implications in a given context (Pressly and Afflerbach, 1995).

While comprehension considers whether a reader can understand the intended meaning of a text and readability refers to the ease with which a reader can understand written text, neither of the two domains of written communication can be evaluated without the other. Therefore, mechanisms that serve to dissect readability must be evaluated as well. These take the form of what is scientifically known as Critical Discourse Analysis (CDA) and is accompanied by proven methods and rubrics.

2.3 Critical Discourse Analysis (CDA)

It is important to understand that inherently, text (or policies for the purposes of this study) are not neutral, but do contain philosophical positions, power dynamics and interest embedded within them (Janks, 1997). Therefore, proven methods must be used to analyse the text and its associated properties or metadata (the information supporting or adjunct to the policies as well as any characterizing properties). This is done such that a complete and comprehensive understanding of the policies are formulated. These methods must remove biases, confusion, and assumptions to ultimately communicate policy intent clearly (Machin and Mayr, 2012).

The analysis of the way in which language is used, to convey messages therefore becomes pivotal in such methods and analysis. Hilary Janks pointed out that Discourse Analysis (DA) stems from a critical theory of language, which sees the use of language as a social practice. This analysis must consider pretexts, errors in composition, perspective, and patterns within the social construct to communicate the underlying message (Janks, 1997).

Assessing the readability and comprehensibility of an information security policy by itself does not necessarily produce any indication of the quality of intent for said document. An analysis of just readability and comprehension is deemed incomplete unless the overall resolutions conveyed are assessed as well. Methods to analyse the inherent intent of a document are broadly called Critical Discourse Analysis and for the purposes of this study, information security documents specifically. This methodology and practice is largely attributed to sociolinguistic studies with major contributions attributed to Norman Fairclough (Fairclough, 2001) and Ruth Wodak (Wodak and Meyer, 2001) as well as Hilary Janks (Janks,1997).

Critical discourse analysis aims to use several methods to critically analyse the actual message, which include an investigation into the tone, intent and language used to convey a message. Discursively, critical discourse analysis has been expansively used in linguistic practice, but more recently, with globalisation and organisations expanding across borders, the application of the methods has seen prominence in social sciences, anthropology, and politics as well as within the field of medicine (Lupton, 2010).

Fairclough has detailed an approach for textual analysis with the outcome of presenting a view of the effectiveness and capability of the document/ text in conveying the inherent and explicit intent. The application of the model to study documents, take the form of an analysis for the inter-related dimensions of discourse (Janks, 1997). Of noting, is that any discourse analysis method used, must adequately dissect a documents' characteristics in terms of social and political inequality as well as to further understand power abuse and/or domination (Fairclough, 2007; Fairclough, 2001). The methodology itself considers characteristics within the grammar and vocabulary of the document. Simply, the methods considers whether the language, tone, grammar, and other variable positively impact the "landing" of the policy intent on its intended audience or creates barriers to it.

The analysis of policies therefore relies on a comprehensive interrogation of all the characteristics used in the compilation of the material, but also on all facets internalized in the actual texts themselves, either through explicit deliberate effort or any implicit characteristics as well.

To analyse the readability of documentation and specific to this study, the readability of IT security policies, it is pivotal to use a mechanism that is scientifically proven. In-spite of the application of Critical Discourse Analysis, a result must be measured somehow, or the analysis is purely subjective and relies on the bias of the person conducting the analysis which may include a number of factors such as own intent, perspective, knowledge, education and other environmental and extraneous variables all of which will obviously greatly influence the outcome.

Therefore, a standardized approach or approaches must be used that are not only proven, but comparable across domains where the method/s have been peer reviewed and are considered robust and universally applicable.

A proven scientific method of assessing readability of any written media and widely considered to be a foremost in this field remains that of Fry's Readability Formula and its resultant graph which categorize a documents' ease of being read and understood according to varying levels of literacy (Fry, 1989; Courtis, 1995). This is because comprehension and understanding of documented organisational policies and procedures rely heavily on literacy levels which may vary significantly within a given country, locale or for the purposes of this study, an organisation as well.

2.4 Fry's Readability Formula

Fry's Readability Formula is widely used across a number of industries and sectors by regulators to ensure that legislation, laws and practices can be understood by the intended audience not only locally (Wissing, Blignaut and Van den Berg, 2016), (Sibanda, 2014), (Snyman, 2004), (Moodley, Pather and Myer, 2005), (Badarudeen and Sabharwal, 2010) but internationally as well with studies conducted across fields (Doak et al., 1998), (Taylor-Clarke et al., 2012), (Ojha, Ismail and Kuppusamy, 2018) (Nietzio, Naber and Bühler, 2014) as well.

The tool examines three 100-word excerpts from the assessed document/s which are then plotted on the Fry readability graph. When plotted, the results generate the level of readability required for the document. This method does not seek to analyse the entire document and is considered a reliable and repeatable measure of a documents' ability to be read and understood (given varying levels of interpretation). Essentially the instrument

samples text from the document, with the result categorising the document as a whole, without the need to analyse the document in its entirety.

The entire document is not analysed as no value is derived from such an exercise simply because the style and intent of a document typically remain consistent throughout in spite of it being authored by one or many subject matter experts and subject to numerous revisions over the course of its' lifetime. Essentially, with more authors, revisions and changing technology constructs, the document is likely to become more "disjointed" and less homogenous over time. Therefore, the assertion is that sampling the document is considered reliable to produce a viable result versus reviewing the entire document (Fry, 1989).

Figure 2.1 below is a graphical representation of the Fry Readability Formula which maps the average number of sentences per 100 words on the Y-axis against the average number of syllables per 100 words on the X-axis. The resultant intersection of these axes informs the Grade level of reading required for the sample 100-word text in Grade level from 1 to 15.

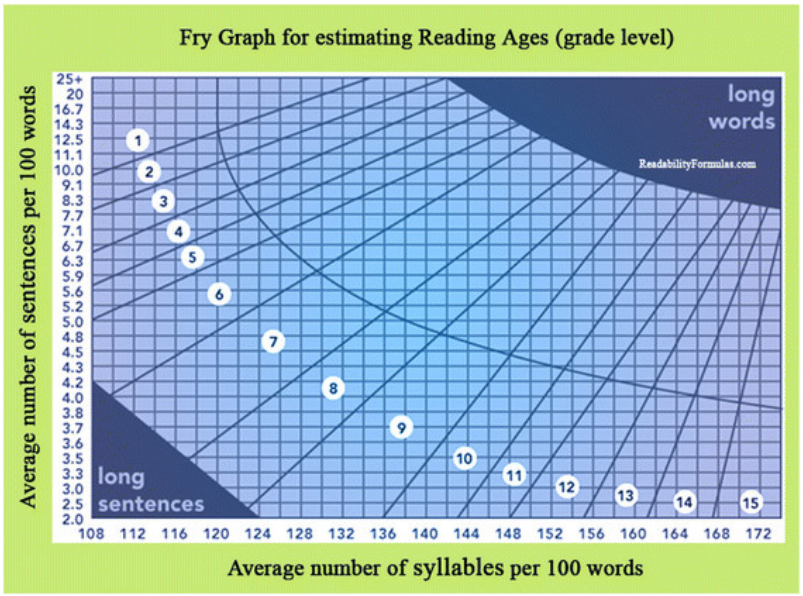

Figure 2.1: Fry's Readability Graph. Source: https://readabilityformulas.com/fry-graph-readability-formula.php.

The ideal use of the model involves the use of between 300-600 words with 600 as an absolute maximum. Noteworthy through this model, is that texts with multisyllabic words

are indicative of text complexity, affecting readability. Moreover, it has been found that words exceeding 3 syllables are classified as difficult words, thus contributing to the difficulty in comprehension in certain circumstances and literacy levels. Therefore, the use of Fry's formula advocates that longer words are substituted by shorter, more common words except where the longer word is familiar to the audience or absolutely necessary to the message/intent (Snyman, 2004).

Fry's Readability Formula and its resultant graph is based on literacy levels of English home language speakers in the United States of America (USA) (Sibanda, 2014). This formula also characterizes additional language speakers to be one grade behind. While not a specific South African model, the result from the formula application can be extrapolated in the local context. Essentially, the output of the formula will result in a grade of literacy level directly applicable to an American English home language reader and speaker. The South African result will be considered to be one level behind.

While the readability formulae can be universally applied to any written text, there are limitations (Redish, 1981) as mentioned above. Given this factor alone in a South African context, further supporting methods of analysing the policies and procedures given the disparity (Dorner and Gorman, 2006) in literacy levels between developed and developing nations is necessitated and required. Not only this, but researchers within CDA consider the use of multiple methods to be more reliable (Wodak and Meyer, 2016). One such mechanism, is the Cloze deletion test.

2.5 Cloze Deletion Test

Another supporting model used to analyse readability of documents is the Cloze test or Cloze deletion test (Taylor, 1953). Using this method, every fifth word of the first 250 words of a document are replaced with blanks and study subjects are asked to guess-replace them contextually. Accurately guess-replaced words indicate in-text cohesion will result overall in higher comprehension and are an indicator of the ease of readability. Textual cohesion indicates an inherently highly readable document while conversely, high rates of inaccuracy in the guess replacements of the deleted words are an indicator of poorly written, complicated, jargonized and/or confusing texts, and in this case policies (Alderson, 1979).

It is important to note however that a study subjects' ability to accurately guess replace the word is a function of a number of characteristics, namely education level, proficiency of subject matter knowledge, familiarity with policy intent, inferred characteristics within the policy, repetition and overall document simplicity and textual cohesion.

Ultimately, the Cloze test (Taylor, 1953) results in a score calculated as a percentage of the correct answers. Limitations of the Cloze test importantly include a result which does not cater for the communication of complex technological concepts (Entin, 1986).

Since complex technological concepts are widely expressed in information security policy, this limitation is noteworthy in terms of this research. Guessing the missing words, when the missing words may be completely new or complex from a technological point of view would create another dimension of complexity to the pure readability of a policy.

Jargon and acronyms are now widely accepted as commonplace within the information security domain with industry professionals coining new terms regularly (Paulsen and Byers, 2019). Consequently, the utilisation of the Cloze test, since it requires participation from respondents, will enhance result outcomes from the study while noting its limitation. Both tools, Fry's and the Cloze test used together will inform an overall, more reliable result around readability.

Given the specific and specialised nature of information security and its associated sciences as well as its accompanying lexicon (Furnell and Bishop, 2020), readability measures must perform reliably and consistently without much disparity in results to create meaningful outcomes.

As is evident, the utilization of simply one rubric is not comprehensive and therefore the utilisation of more than one model to assess the readability of a document is not only prudent, but further informs the assessment around the policies' effectiveness. While the models do have limitations in application and outcomes as well as the extrapolation thereof, a combination of models and quantitative analysis will yield a reliable result as to the policy effectiveness from a readability and operationalization point of view. It is for this reason that a critical discourse analysis tool which accounts for the limitations of the Cloze test (i.e., technological concepts) is used as well.

2.6 The Simple Measure of Gobbledygook (SMOG)

The Simple Measure of Gobbledygook (SMOG) (McLaughlin, 1969) is another reliable method to determine the reading level required for written material. The SMOG method involves counting 10 sentences at the start of the subject material as well as the middle and near the end. Counting every word with three or more syllables in each sentence grouping even if the same words recur is required. The total number of counted words are then mapped on the SMOG Conversion table to establish the reading level required. While the rules for calculating inclusion or exclusion of words are complicated, the model itself does produce meaningful outcomes (Leonard Grabeel et al., 2018) and is considered useful where jargon is commonplace, as is common with information technology and more especially, the domain of information security (Lenzini et al., 2014; Bratus, et al., 2016).

The following table is the SMOG conversion table displaying the categorisation of total word counts and corresponding Grade Level required. Additionally, the table includes the number of sentences with the applicable conversion number.

SMOG CONVERSION TABLES			
SMOG Conversion Table I > 30 Sentences		SMOG Conversion Table II <30 Sentences	
Word Count	Grade Level	No. of Sentences	Conversion No.
0-2	4	29	1.03
3-6	5	28	1.07
7-12	6	27	1.1
13-20	7	26	1.15
21-30	8	25	1.2
31-42	9	24	1.25
43-56	10	23	1.3
57-72	11	22	1.36
73-90	12	21	1.43
91-110	13	20	1.5
111-132	14	19	1.58
133-156	15	18	1.67
157-182	16	17	1.76
183-210	17	16	1.87

SMOG CONVERSION TABLES			
SMOG Conversion Table I > 30 Sentences		SMOG Conversion Table II <30 Sentences	
Word Count	Grade Level	No. of Sentences	Conversion No.
211-240	18	15	2.0
		14	2.14
		13	2.3
		12	2.5
		11	2.7
		10	3.0

Table 2.1: SMOG Conversion Table.

Source: Derguech, Zainab and D'Aquin, 2018)

While a readability analysis will indicate the readability of IT security policies in use within the organisation given the use of a combination of Fry's readability graph, the Cloze test as well as the SMOG test, it is prudent to consider the message itself, or in other words, the inherent intent of the information security policy.

This then informs and analyses the overall expected outcomes of the policy for the target audience as in many cases, the intent itself may be explicitly technical in nature (Holmes, 2001) and is sometimes not easily or succinctly communicated. Critical discourse analysis involves considering not only output from the tools, but what the organisation is trying to communicate ultimately. This would indicate that even though the policy may be rated as requiring high levels of reading literacy, it may be possible for the actual intent to still be communicated. Therefore, analysing policy outcomes and measuring same will inform a more holistic and robust critical discourse analysis. Therefore, the use of a mix of quantitative methods and qualitative methods will yield more reliable results.

The converse is also true in that documents rated as requiring low levels of literacy or reading capability may still be inadequate at communicating policy intent properly. This ultimately results in a varied view or understanding of information security policy intent within the organization and as a result, will result in differing levels of compliance to said policies and procedures in practice as a natural consequence.

The unfortunate outcome of the above is impaired understanding and this therefore results in technology choices and decision-making occurring in limited contexts and applications, or not considering all policy implications. This then places staff who are information security professionals or subject matter experts in the position of constantly explaining what the policy stipulations mean in committees, meetings, forums, and other documents as well as in communication to vendors and 3rd parties. This clearly underscores the importance of policies and procedures that are easily understood by the layman (non-technical staff) as well as experts in the domain so that the intent is cohesive and universal in its application at levels of the organization.

Information security as a practice is by no means new or in infancy by any measure. Industry bodies and working groups are common, seeking to govern, standardize and formalize the approach to information security management in the public and private sectors. This has resulted in the formulation of standards, frameworks, and implementation guides for information security as a domain by itself seen as independent of information technology (Dhillon and Backhouse, 2001).

Within the Information Security domain, the ISO (International Standards Organisation) standard for Information Security is called ISO27001:2013 and has established itself as "The" standard in enterprises (Boehmer, 2008).

2.7 ISO 27001 and the Information Security Domain

ISO 27001 is an international standard for information security management systems (ISMS). It defines the requirements for the implementation of an Information Security Management System (ISMS) and was developed by the International Electrotechnical Commission IEC Technical Committee (IEC JTC). It provides an encompassing and systematic approach for organizations to establish as well as implement, maintain, and continually improve their information security practice or programme. The standard itself defines a framework which enables organisations to manage and protect sensitive information, ensuring its' confidentiality, integrity, and availability. ISO 27001 is widely recognized and adopted globally, serving as a benchmark for information security management (Björnsdottir et al., 2022).

ISO 27001 has achieved significant international and local acknowledgement and uptake, making it one of the most widespread standards in the field of information security. Organizations across varied industries, including finance, healthcare, government, and technology (have all embraced ISO 27001 as the de-facto fundamental framework for managing their information security programme. This wide-scale adoption confirms the standard's relevance as well as applicability in different contexts (Aljabre, 2020; Nowatzki & DaVeiga, 2019).

The implementation of ISO 27001 requires organizations to assess their information security risks, identify applicable controls, and establish a comprehensive ISMS (through meticulous planning, defining, documenting, communicating and ongoing measuring). While the degree of implementation varies across organizations, research suggests a growing trend of successful ISO 27001 implementations (Aljabre, 2020; Nowatzki & DaVeiga, 2019).

Organizations that have fully embraced the standard often report improved information security posture, increased customer confidence, and enhanced regulatory compliance as an inherent outcome associated with its' implementation. it is therefore vital to acknowledge that implementation challenges may arise, such as resource constraints, lack of management commitment, and difficulties in integrating the standard with existing processes (Ruohonen and Siponen, 2019; Cepeda-Carrion et al., 2020) within the organisation. This results in an impaired implementation and can have significant negative consequences.

ISO 27001 is important within the domain of information security since it provides a holistic and systematic approach to manage information security risks and protect valuable data. It emphasizes the importance of maintaining confidentiality, integrity, and availability of information, which are critical for business operations and maintaining stakeholders' trust. ISO 27001's focus on risk management and continual improvement aligns with a constantly evolving threat landscape and the resultant need for organizations to adapt their security measures on an ongoing basis. Additionally, ISO 27001 certification can serve as a competitive advantage, demonstrating an organization's commitment to information security and enhancing its reputation within the industry sector it operates (Aljabre, 2020; Nowatzki & DaVeiga, 2019).

ISO 27001 itself can be viewed as discourse created around the domain of information security as a discipline. Framed in this manner, it is then essential to consider its contribution to overall security implementation, awareness, and measurement.

ISO27001 itself combines coordinated, coherent, cost effective and comprehensive measures for IT security strategies (Calder and Watkins, 2012). In order to align or adhere to the standard, organisations must:

1. Continuously understand the organizational context. This includes analysing risk, threats, exposure, and resultant impact (SWOT (Strength, Weaknesses, Opportunities and Threat analysis)) (Farn, Lin and Fung, 2004).
2. Formulate and adopt information security controls to address identified risks and threats. This results in deliberate measures to manage and monitor these threats and the organizations response to same.
3. The implementation of a process to assess the capability of response and cost/risk against these threats on an ongoing basis. This is viewed as the continual improvement factor in ensuring controls are fit for purpose, simple, align with industry standards both in the domain as well as the sector as well.

The standard itself is founded on 10 brief clauses which advocate the requirements for a properly functioning security strategy including the implementation of an ISMS (Information Security Management System), but include a much more detailed annexure (A) which provides more comprehensive control sets, divided into 14 sets, they are (ISO, 2022):

1. Annex A.5- Information Security Policies (2 Controls)
2. Annex A.6 – Organisation of information security (7 Controls)
3. Annex A.7 – Human resource security (6 Controls)
4. Annex A.8 – Asset management (10 Controls)
5. Annex A.9 – Access control (14 Controls)
6. Annex A.10 – Cryptography (2 Controls)
7. Annex A.11 – Physical and environmental security (15 Controls)
8. Annex A.12 – Operations security (14 Controls)

9. Annex A.13 – Communications security (7 Controls)
10. Annex A.14 – System acquisition, development, and maintenance (13 Controls)
11. Annex A.15 – Supplier relationships (5 Controls)
12. Annex A.16 – Information security incident management (7 Controls)
13. Annex A.17 – Information security aspects of business continuity management (4 Controls)
14. Annex A.18 – Compliance (8 Controls)

Specifically, Annex A5 which has 2 controls listed applicable to policy is relevant.

- 5.1.1 Advocates that all information security policies are approved, published, and communicated to relevant external parties.
- 5.1.2 Indicates that policies must be regularly reviewed or where significant corrections are made to ensure the policy remains consistent with the organisational threat environment, regulations, and objectives.

Given the wide adoption, applicability and implementation of ISO 27001, it is problematic that while there are 2 controls specifically about policy, there are no control guidance details around the actual information security policy formulation or the communication thereof. Essentially, what is widely considered to be the single most important guidance document for information security, contains no actual guidance or controls to guide the creation of the policy itself. Additionally, the guidance does not indicate any guidelines around language, jargon, acronyms, or complexity. This is possibly due to the universal and scalable application of the standard in its implementation worldwide. There are no mandatory components to the policy and while thousands of templates are available online (in generic format), which must be crafted and tailored to suit an organisations specific attribute, there exists no documentation around the composition of the policy itself or characteristics/ components to be avoided.

This does leave the finer details up to the organization to decide and cater for the individual requirements, local laws, regulations, and organizational maturity where policy implementation is concerned. Essentially the standard allows creative license in terms of making sure the policy is capable of communicating security intent. This failing

potentially creates instances where an organisation may not be aware of readability and comprehension within the wider context of CDA and omit the inclusion of its directives and imperatives. This omission then leads to weak and inadequate documentation of policy and policy intent. This has the unfavourable consequence of then creating ambiguity by design.

As a consequence, information security policies are then poorly constructed, complicated and difficult to understand. Although this is something that is entirely within the organisations' control to rectify and cannot be ascribed to the technical nature of the information security domain. Essentially, there is nothing at all that prevents an organization from defining, implementing, and reviewing simple and robust information security policies from the outset and not utilising CDA and its constructs potentially inclines a document to inherent inadequacy. It is possible however for an organisation to "get it right" purely incidentally and this possibility cannot be discounted although, unlikely.

Of noting is that the updated standard ISO27001:2018 contains 77 terms and definitions explaining a number of words and phrases. While this is not unusual in any manner, what is important is that even an information security standard meant to be universal and all-encompassing for widespread adoption contains an exhaustive list of terms and abbreviations and their accompanying explanations.

This further demonstrates the challenge faced with simplifying information security policy and domain knowledge to the point that the original intent and message is conveyed but abstracted enough so as not to confuse and alienate the reader or implementer. While it is true that information security is a specialised domain of knowledge just like any other, it is also true that information security is applicable to any user of information, which is considered pervasive today.

Often, policies are written from the very specific context and perspective of the subject matter expert and then subjected to numerous review iterations by other subject matter experts (Siponen and Vance, 2010). While this is an important and often overlooked step in policy creation, it is not an exact science and miscommunication still exists. In the context of information security policies, this is especially problematic since

misconception and ambiguity can easily result in failed information security controls ultimately leading to a failed ISMS implementation and security programme and consequently results in financial or reputational loss (Hameed, et al., 2013; Cavusoglu et al., 2004).

2.8 Existing research on Information Security Policy Readability

In the analysis of existing research on information security readability and the implications, it was found that research has focused heavily on information security policy design, including the aspects which must be taken into account which include the "what, how and who" (Flowerday and Tuyikeze, 2016) as well as referencing the Deming cycle of Plan, Do, Check, Act (Velasco et al., 2018) where it pertains to ensuring that an information security policy is subjected to ongoing review and analysis.

Further to this, it was found that research has concentrated on ensuring that information security policy is aligned to organizational strategy (Alshammari et al., 2015; Johnson et al., 2007) with a focus on aligning to the concepts in the ISO standards family (seen as best practice) as well as evaluating whether the information security policy is aligned to the ISMS defined at the organization or through the industry sector the organization is located within (Doherty et al., 2006).

Reasons as to why ISMS implementations potentially fail are often attributed to weak commitment from management (AbuSaad et al., 2011), an implementation that is not fit for purpose, for the industry or sector, or laws are conceptually adhered to, but not necessarily brought into force via the ISMS and lack of coherence in ensuring the policy is actually implemented resulting in breaches and data or financial loss (Dombora, 2016).

Research into policies titled "Information security policies: A review of challenges and influencing factors" reviews academic literature and reports of information security institutes relating to policy compliance. The research investigation concludes that non-compliance with information security policy is one of the major challenges facing organizations and that this is primarily considered to be a human problem rather than a technical issue (Alotaibi et al., 2016). If the problem is identified as human versus technical, the components are likely to be inadherence to the policy, ignorance or

deliberate avoidance of the rules and common practices communicated via information security policy.

This creates an environment where employees potentially fully intend to comply with information security policy during their daily duties, but information security failures persist. Further to this, investigations as to why policy violations persist, called "Research: Why Employees Violate Cybersecurity Policies" found that during a 10-day study period, 67% of participants reported failing to fully adhere to cybersecurity policies at least once. The top three reasons given for failing to follow security policies were "to better accomplish tasks for my job," "to get something I needed," and "to help others get their work done" (Posey and Shoss, 2022). Given the reasons disclosed, there is no indication of wilful negligence or malfeasance. Employees fully intended to comply but during the daily performance of tasks, did not. This informs a view that creating policies, communicating them widely and employees reading them does not equate to compliance and that non-compliance rates are potentially significant.

Seemingly inane, these non-compliance incidents on an ongoing basis with policies could include, but are not limited to sharing passwords, weak cyber hygiene and unsecured applications, data and services that are left exposed inadvertently. These are then exploited by hackers and those with malicious intent (Weak Security Controls and Practices Routinely Exploited for Initial Access, 2022).

Essentially, information security policies are documents that define the rules and principles for protecting the information assets of an organization. They are essential for ensuring the confidentiality, integrity, and availability of information, as well as for complying with legal and regulatory requirements.

However, they are often ineffective if they are not well understood and followed by the end-user. Therefore, it is important to analyse and evaluate the readability and comprehension of these policies, as these factors may influence the user's behaviour and attitude toward information security.

Readability is the ease of understanding a written text, while comprehension is the ability to grasp the meaning and intention of a text. Readability and comprehension are affected

by various factors, such as the vocabulary, syntax, structure, layout, and style of the text, as well as the background knowledge, motivation, and interest of the reader. Researchers have designed a number of readability metrics that evaluate how difficult a passage is to comprehend based on some linguistic features, such as word frequency and sentence length.

However, these metrics alone have limitations and challenges when applied to information security as they do not account for the domain-specific terminology, the complexity of security concepts, and the variability of user backgrounds and preferences (Perez-Guillermo, 2015) especially noteworthy in the South African context .

Several studies have attempted to investigate the impact of readability on the interpretation of information security policies and to identify if readability metrics can be used to assess the difficulty of information security documents. For example, Alkhurayyif and Weir (2018) examined and compared eight information security policy documents on nine mechanical readability formula results with outcomes from human-based comprehension tests and found that traditional readability metrics were inadequate alone.

Specific to the context of this specific study, an important reason why ISMS failures result is as a consequence of readability and comprehension issues identified within the documents themselves (Plate, 2011). In this study by Plate (2011), the researcher proposed a management framework for information security based on the ISO/IEC 27001 standard. The framework included a process for evaluating the readability of information security policies using various readability metrics and tools. The study suggested that applying readability metrics may allow policy designers to evaluate their draft policies for ease of comprehension prior to policy release. The study also recommended further research on developing and validating domain-specific readability metrics for information security policies.

These studies indicate that readability is an important factor in information security policies and that software readability metrics can provide some insight into the likely difficulty that end-users face in comprehending an information security document. However, there is still a need for more research on developing and validating domain-specific readability metrics or scope to develop such metrics that are specific to the

security domain. This includes, but is not limited to the design of conceptual or theoretical frameworks which can then be adopted or further studied resulting in an advancement in this body of knowledge.

One of the main challenges in analysing and evaluating the readability and comprehension of information security policies is the lack of standardized methods and criteria for measuring these factors. Different studies may use different readability metrics, comprehension tests, documents, and user samples, which may affect the validity and reliability of the results.

Moreover, some studies may not report sufficient details about their methods and data analysis procedures, which may limit the replicability and generalizability of their findings.

Another challenge is the complexity and diversity of information security concepts and terminology, which may pose difficulties for both critical discourse readability metrics and human readers. Critical discourse metrics may not be able to capture the semantic nuances and contextual meanings of security terms, while human readers may not have adequate background knowledge or interest in security topics.

Therefore, it is important to consider both syntactic and semantic aspects of readability and comprehension, as well as to provide clear definitions and explanations for security terms.

A third challenge is the variability and subjectivity of user backgrounds and preferences, which may influence their perception and interpretation. Users may have different levels of education, experience, motivation, attitude, culture, language, etc., which may affect their ability and willingness to read and understand the documents. Therefore, it is important to consider the user's perspective and feedback when designing and evaluating information security policies, as well as to tailor the discourse to suit different user groups, where it is possible to do so, and feasible.

In conclusion, information security policy analysis and evaluation are crucial for ensuring the effectiveness and compliance of information security policy. Readability and

comprehension are key factors that affect the user's understanding and behaviour toward information security. However, there are many challenges and issues that need to be addressed when measuring these factors. Further research is needed to develop and validate domain-specific readability metrics for information security policies, as well as to explore the syntactic, semantic, and pragmatic aspects of readability and comprehension within the information security domain.

In addition to this, is the fact that while there are various reasons for breaches, when they do occur, a problematic ISMS is attributed (Hayeri Khyavi and Rahimi, 2015).

2.9 The Conceptual Framework

Given the current research on readability of information security policies in the organizational context and specifically the implications this has on ISMS and its implementation outcomes, a conceptual framework is presented to underpin this study. This framework is illustrated in Figure 2.2.

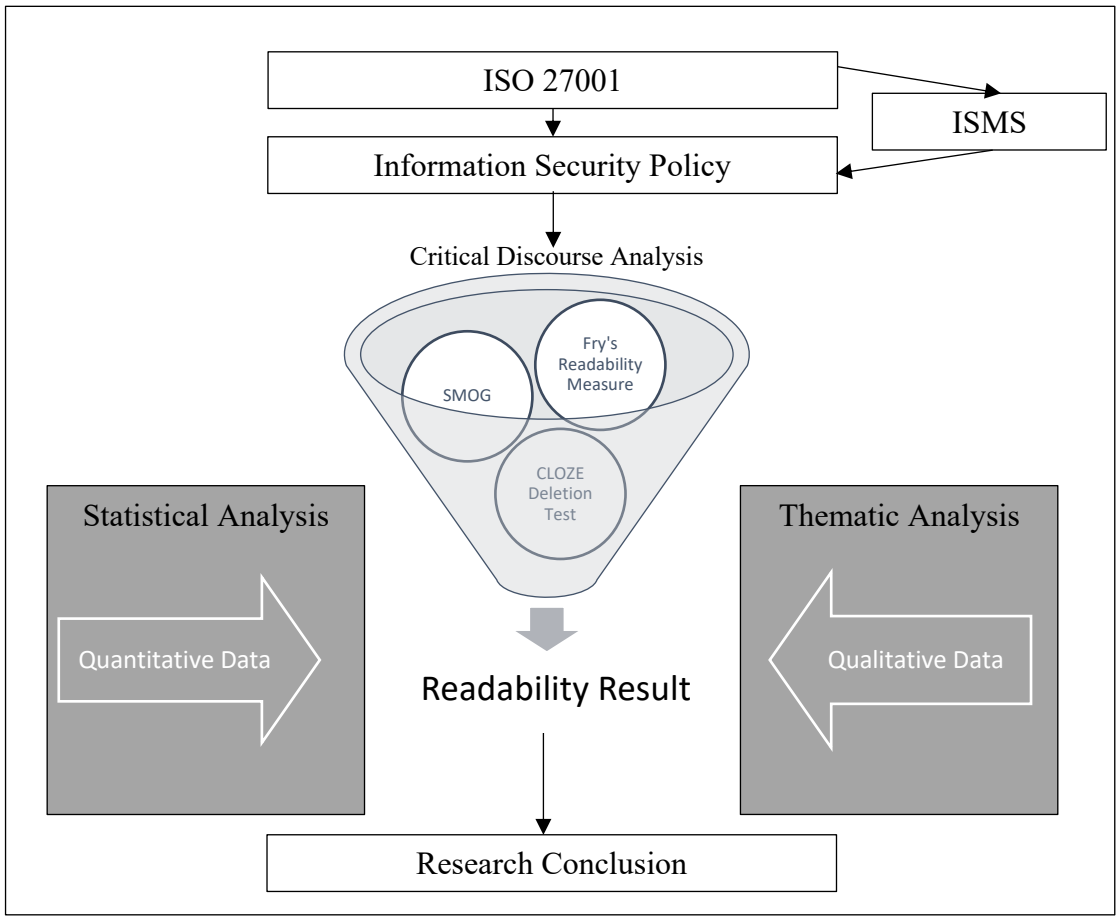

Figure 2.2 Conceptual Model for study

Figure 2.2 represents the primitive factors impacting and impacted by the studies variable and overall, informs the methodology and mechanism with which the study has been completed. ISO27001 and the existing body of knowledge inherent in the standard as well as its underlying concepts inform the creation of an ISMS within the organizational context which then results in the documentation, review and communication of an Information Security Policy. This is then subjected to the rigor of Critical Discourse tools such as that of Fry, Cloze Deletion and the SMOG Index ultimately informing a readability result which is analyzed within the context of quantitative analysis (from data collected in surveys) as well as further within the context of qualitative data (from themes highlighted out of interviews). This ultimately culminates in an outcome which informs the research conclusion of the study.

2.10 Conclusion

This Chapter has provided an overview and analysis of the existing research and analysis in understand policy setting from an information security point of view. Additionally, an introduction into Critical Discourse Analysis has been provided and its ramifications and importance in understanding defining and characterizing factors in written communication. The methods used to dissect source material such as Fry's Readability as well as the Cloze test and SMOG measure have been introduced and analysed for its applicability to this study and possible shortcomings and limitations have been examined. Finally, the ISO 27001 standard and its subset documents, standards and annexures have been introduced especially where policy setting, and information security intent is communicated within an organization.

Within the realm of information security policy analysis, a notable gap exists in the application of Critical Discourse Analysis (CDA) as an analytical framework for interrogating policy documents. Despite the expanding significance of information security policies in safeguarding and ensuring organizational resilience, there remains a lack of comprehensive studies that engage CDA to scrutinize the underlying discourse as it pertains to information security as a discipline. Existing research predominantly concentrates on technical and procedural aspects, largely overlooking the intricate interplay of power dynamics, ideologies, and socio-political factors encompassed within the textual context of information security policies. This gap is further highlighted by the absence of specific and detailed investigations into how language resultantly constructs

as well as shapes the discourse surrounding information security, ultimately influencing policy comprehension, compliance, and effectiveness.

In addition, the existing literature on the conjunction between CDA and information security policy analysis exhibits a superficial inclusion of cross-disciplinary perspectives. Despite the interdisciplinary nature of information security, most studies tend to adopt a siloed approach, predominantly anchored in linguistics or information technology domains, and sometimes exclusionary in nature. This compartmentalization has constrained the complete exploration of how diverse knowledge domains, such as linguistics, sociology, and information management, converge to explain rationally, the inadequacies that are often inherent in the policy and textual discourse, but also through the communication and socialisation mechanisms as well. As a consequence, an integrated and inclusive framework for critically analysing information security policies is conspicuously absent, and has been developed in this study. This deficiency impairs a comprehensive understanding of the policy documents, their rhetorical functions, and the potential implications for stakeholder engagement, organizational culture, and cybersecurity practices. Consequently, a pivotal research gap persists at the intersection of CDA and information security policy analysis, necessitating analysis using available mechanisms either quantitative or qualitative in nature. This ultimately informs a reliable outcome supported by statistical analysis creating actionable imperatives for implementation and further study.

CHAPTER 3

Research Methodology

3.1 Introduction

Research is performed primarily to find novel solutions to problems or answer questions (Hartz-Karp and Marinova, 2017). The results of which, add further depth to existing bodies of knowledge in a chosen field and provide insight into the problems, or challenge existing views on the subject matter.

When conducting research, it is vital to use carefully considered approaches, methods, and where possible, statistically reliable tools, so that results can be verified, replicated, and challenged to create robust outcomes.

In this chapter, the underlying philosophy, approach, data collection mechanisms, techniques as well as shortcomings and other considerations will be detailed.

3.2 Research design

To conduct this research, the various available research methodologies are considered, which must cater for the various research instruments such as surveys and questionnaires as well as using readability constructs such as that of Fry, SMOG and Cloze which are to be employed. Surveys are defined as quantitative methods for research analysis (Saunders, Lewis and Thornhill, 2018) and interviews as qualitative in nature (Jamshed, 2014). Therefore, since the resulting data will consist of both quantitative and qualitative data, a mixed-method approach will be taken (Creswell and Creswell, 2018).

3.3 Research methodology

For this study, the underlying approach used relies on the mechanism called the Research Onion (Saunders and Tosey, 2015). This model outlines the approach to be taken to conduct research and involves an outside in or peeling of the layers. Essentially, the approach advocates the gradual intensification of analysis as a study progresses as indicated below in Figure 3.1:

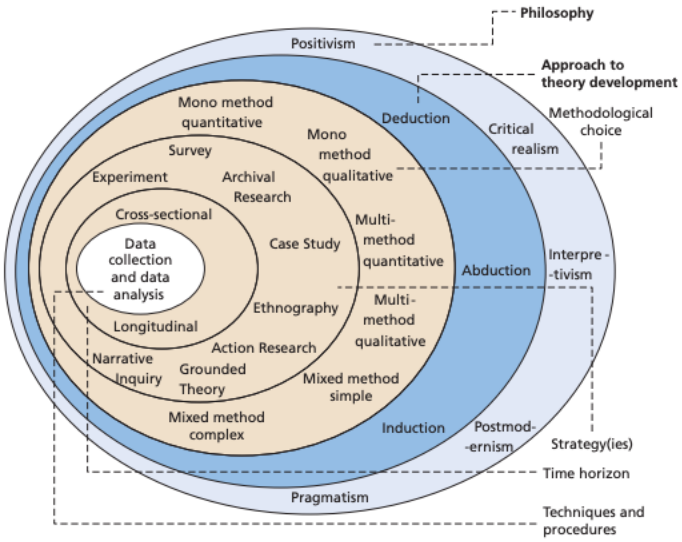

Figure 3.1: The Research Onion. Source: Saunders et al., 2015.

The Onion provides an approach for research to be conducted by first creating a philosophy which is then expanded into a strategy, thereafter an approach to theory development is performed which informs the methodological choice.

This is then expanded further into more detailed strategies which drive the time horizon for the study and ultimately result in the formulation of approaches to data collection and analysis.

The use of a mixed-methods approach enabled the attainment of more complex views that would simply not be possible using only surveys and questionnaires (Creswell and Creswell, 2018). Therefore, and in an effort to present more significant outcomes from the data as well as to ensure limitations present in surveys or questionnaires alone are not carried through in the research, interview data was combined to enrich the data overall. Interviews were chosen since the following characteristics can be exploited:

- Forces a direct approach and the ability for clarifying questions to be asked versus relying on assumptions made in surveys.
- Focusses on a narrow topic and sparks other ideas and outcomes which may not be obvious immediately in a survey.

Within the context of this research mixed-methods approach was selected so that a more nuanced understanding of the research problem was possible. In addition, mixed-methods approach does facilitate a more detailed understanding of the connections and contradictions possible between qualitative and quantitative data and enables questions to be answered more deeply (Almeida, 2018). Moreover, the limitations of single methods are balanced out yielding deeper insight while also allowing more flexibility in designing the research instruments (Shorten et al., 2017) which was relevant to the context of this study. The organisation studied while not averse to being studied, did present some challenges in that all staff chosen to participate in the survey did not ultimately participate and many opted out given "research fatigue" which was commonplace with remote studies conducted during social distancing and COVID lockdowns. Moreover, many saw the research as "audits" further disinclining them to participate. Ultimately the mixed-method approach yielding adequate data to inform the analysis phase of the research, and rich data to answer the research questions.

Conducting this mixed-methods study was not without pitfalls in that the complexity was significantly increased given the magnitude of data from each of the data sources. Further, it was possible that bias was introduced where survey results could be favoured over interview data or vice versa and therefore the researcher was careful to present the data clearly and used statistical methods to proof the data for its viability to be included in the study especially where the data was materially significant.

3.4 The research philosophy

At a very basic level research philosophy is the overall belief and views-based system for investigating concepts and things (Saunders and Tosey, 2015). Essentially comprising four philosophies, they are categorized according to their nature.

Pragmatism is the combination of many methods for gathering data and informs an outcome that is best for research that utilize both qualitative and quantitative methods to understand the problem.

Interpretivism, relies on detailed data gathering on the problem characterized by smaller samples and ideally suited toward qualitative research.

Realism on the other hand is an approach rooted in scientific methods of inquiry.

Positivist philosophy, like realism, uses scientific methods to test theories and is characterized by larger samples in comparison to interpretivism. This philosophy allows the researcher to create an explanation from what is observable and therefore allows for extrapolation of data results to much larger study populations overall.

For the purposes of this research, a hybrid pragmatist approach to philosophy is used since a combination of surveys, interviews and scientific methods are used to create an overall view of the comprehensibility and utility of information security policy and implementation within the target research site.

3.5 Research Approach

All policy documents were dissected into subtext that was analysed by Fry's Readability graph as well the SMOG method and Cloze test and the results were plotted on the associated graphs to reflect its readability and usability.

Additionally, to confirm the outcomes from the various readability tests through the models, a further interview process was conducted with another group of interviewees in order to gauge whether the comprehended outcomes align with the policy intent. This was an important step required to ensure that the test (surveys) were compared against a control group (interviews) to either confirm or refute any outcomes from the tests themselves and has provided a more summative view overall with respect to the studies' aims and objectives.

The use of scientifically reliable methods such as the Fry's readability model as well as the SMOG test naturally incline the methodology toward a nomothetic approach which evaluates group norms and views (Monks, 1995). These scientific instruments have been used repeatedly across industries, sectors, and sciences to understand the readability and communicability of policies and procedures.

3.6 Study Site and target population

A large financial services organisation within South Africa provided consent for their IT security policies and procedures to be analysed and studied to understand whether or not these policies and related documents that form a key component of discourse with employees were not exclusionary and/or ambiguous in nature. The researcher is an employee at the organisation and therefore had access to the policies, staff contact details through global address lists and an underlying understanding of the methods and approaches to information security policy being used in the organisation. Since the information security policy is applicable to all employees, contractors, and 3rd party vendors, it is considered universally applicable in the organisational context and all staff at the study site were within scope to participate.

3.7 Sampling Strategies

While there are two distinct sampling techniques, namely probability and non-probability sampling, for the purposes of this study, probability sampling techniques were used so that all members of the population had an equal chance of being selected to participate in the study (Coolican, 2017) instead of non-probability sampling which removes random selection (Taherdoost, 2016). Moreover, the study relied on a total population that is finite or well known.

3.8 Sample size

The calculation of the sample size out of the total population involved the use of the sample size formula created by Naing, Winn and Rusli (2006) where populations are finite. The formula used was:

$$n = \frac{Z^2 P(1-P)}{d^2}$$

Here n= sample size, Z=Statistic for level of confidence, P=estimated proportion or prevalence (If the expected prevalence is 20%, then P = 0.2 and d=precision or margin of error permitted (if the precision is 5% then d=0.05).

The values used in the equation are Z=95%, P=0.1%, d=0.30 %, which resulted in a calculated sample size (n) of 214.

In order to simplify the dissemination of the survey, response collection and analysis of the result, an online survey portal www.surveymonkey.com was used. This provided an accurate view of whether or not respondents were in fact able to replace the missing words in the deletion test accurately and is considered a reliable method to conduct surveys remotely and online (Waclawski, 2012).

In instances where respondents inaccurately guess the missing words in the Cloze deletion test, this indicated a general impairment in the policy construct not only from a design perspective, but would likely decrease the overall likelihood of comprehension as well. This was then overlaid with the results from the SMOG and Fry's readability tables indicating the required education level required. Where the result from the survey indicated that the words were in fact guessed correctly, a view was created that points to a level of understandability required to make the policies effective in delivering the management intent i.e., informing staff as to the use and applicability of information security within the organisation.

Ultimately based on the readability analysis output from Fry's method as well as the SMOG method, rationalised by the Cloze test results, an informed and reliable view in terms of the readability and therefore consequence comprehension could be formulated. Since the Fry and SMOG test are considered theoretical in nature and although proven reliably from an academic point of view, these instruments did not provide a view from the readers perspective. This means that's while the Fry result and SMOG result may indicate a required reading level, it was still possible for the reader to not only read the policy but comprehend the policy as well. Consequently, the results from these tests were, compared to the resultant survey results where participants guess deleted words and is an indication of general understanding of concepts, jargon, tone and prior knowledge all of which assist in the accurate guessing of words. Finally, the interviews yielded opinions the themes which were then analysed in comparison to the readability and deletion results to inform an overall conclusion.

3.9 Data Collection Method

The research method involved mixed methods, including both quantitative and qualitative data (Creswell, 2014). Given the research aims and objectives as well as tools like the Cloze deletion test which were utilised, the study has used surveys and interviews (Shanks and Bekmamedova, 2018) in order to gather the required data. With respect to the survey itself, respondents were required to type in the word independently in a free text box. This served to prevent any bias or indication/preconceived notion around what the word should be. For the guessed word to match the deleted word, it must be the exact deleted word and the researcher ignored misspelling. If the word deleted was a technical term/acronym or abbreviation, then only the exact match was deemed acceptable (Cheng and Warren, 1999). This used the approach of fixed deletion in terms of the Cloze test where every 5th word was deleted and needed to be guessed by the respondent. Rational deletion was not used since the purpose of the test was to understand overall intent versus the intent of specific sentences and therefore provide a summative assessment of the policy instead of simply assessing in-scope sentences that were randomly selected from the entire policy.

All respondents were only permitted to take the survey once by the survey tools' online IP (Internet Protocol) address checking, thereby removing the possibility that staff may repeatedly try to accurately guess the deleted words correctly and all results have remained confidential and not communicated to other staff or line managers.

To ensure that the received response rate was high, 6 full calendar months was allotted for recipients to respond, and all respondents were randomly selected by drawing a staff list of all staff and using the RANDBETWEEN function in Microsoft Excel.

Additionally, and to reduce the time required for the study, the survey response allotted time was run parallel with the processing of policies through the Fry and SMOG tools. This resulted in a total reduction of overall time required to perform the study and created a time buffer in the event that the survey expiration time needed to be extended.

3.10 Researcher biases

It is important to also point out that the researcher performing the study was a full-time employee at the organisation and already held the view that the policies in use were not

readable by all employee levels within the organisation. Consequently, the study was inclined to a bias where the policy intent and effectiveness in delivering the intended message was viewed by the researcher as inherently flawed, although it is possible that the lack of adequate comprehension and readability of the documents could be attributed to a number of other factors, such as race, education level, background and socio-economic factors as well as age, gender, occupation and hierarchical placement and not solely to an impairment in the document itself.

In the context of the Cloze deletion test, various characteristics may impair or improve a respondents' ability to correctly guess missing words in a given text. No bias was introduced into the Cloze test given its design and the manner in which it was designed to be used, however it is important to make the distinction between researcher bias and the instruments being used.

While bias existed from the researcher, it was not possible to introduce this bias into the rubrics of SMOG, Fry and Cloze since these mechanisms are resistant to interference (Van Dijk, 1993). In addition, the researcher did not ask leading questions to respondents. All respondents were only asked the pre-defined approved questions and the researcher only answered clarification questions from respondents. Therefore, the factors impacting the completion of the Cloze survey remain intact, and their influence impairing or improving the correct guess-replacing of words was not affected.

In order to cater for the pre-existing views on the study subject, survey results were used in their original context (Baldwin et al., 2022) in order to arrest bias, since the output from Fry's readability and the SMOG test cannot be manipulated to infer a pre-existing held belief, i.e., that the policies are ineffective. Moreover, results from the interviews provided a balanced view from interviewed staff and worked to counteract researcher bias (Galdas, 2017). A critical review of this study has analysed all results and output displayed from the researcher to ensure that the study remained impartial and the possibility of bias permeating the study was limited.

Bias in research is not to be ignored, researchers must acknowledge any bias and understand the motivating characteristics behind it while developing tools and methods to overcome and robustly challenge this bias scientifically (Montero-marin et al., 2019).

This then produces research results which are far more reliable since the researcher does not work to prove otherwise if results are not what they expect (Grossman, 2021).

3.11 Research format

Essentially the research followed the following format:

1. Policies and procedures under scope were vetted against the Fry readability matrix as well as the SMOG test and results displayed indicating a view of the associated readability and its impact on uptake and readability in the organisation.
2. The Cloze test took the form of a survey where a staff list was used to randomly select the sample out of the population, calculated to be 214 staff. It is important to point out that any number of characteristics my impact the comprehension of a policy document and this has been analysed within the findings. Moreover, while it is possible that a document may be inherently flawed, it could still result in well received comprehension and outcomes from the survey. Since the study relied on all employees having an equal chance of being selected, the randomisation ignored characteristics such as department, designation, level, race, age, sex, remuneration, qualification level and any other characteristic to ensure every respondent had an equal chance of being selected as a study participant. After selection, the participant received communication from the researcher informing them of the study and their selection seeking their approval to participate. If the response was in the affirmative, then the participant received the online link for the completion of the Cloze deletion survey. If the response was negative, indicating that the participant did not wish to participate, they received a response confirming that they will not receive further communication from the researcher. This then resulted in a new participant being selected from the staff list and the process was repeated until all 214 available “slots” for participants were requested.
3. The next step in the study involved an interview of another set of participants, considered an independent group. Out of the sample of 214 participants, 20% of respondents was 42.8 participants, therefore 45 interviews were conducted on another group using open questions designed to gather information about the effectiveness of the policies, understandability, and use. The 45 participants were

selected randomly again using the method described above and were asked the questions in a 45-minute interview. Due to the impact of coronavirus, these interviews were conducted virtually using Microsoft Teams, to which all staff had access and were familiar with. Since the outbreak of the virus, most staff had been working remotely since Mid-March 2020 depending on government and official guidance and as a result conducting the interviews remotely proved more efficient and was anticipated to reduce negative response rates to participate. The interviews were then transcribed into appendices in the study, but most importantly, these interviews and the answers then yielded important views as to the applicability, use and entrenchment of the policies within the IT and general context. The interview outcomes were then grouped into themes and viewpoints and presented in the study results.

4. Juxtaposing the Fry readability scores of the policy, the survey responses to the Cloze deletion test and the views expressed openly via the interviews then yielded an outcome determining the conclusion and informing valuable concepts and confirming or refuting the hypothesis regarding the readability and implied comprehension of the policies in conveying IT security intent and implementable measures as well as insight specific to conceptual ideas around communication and awareness of said policies.
5. Finally given the outcomes in terms of themes emanating from the interviews conducted as well the results from surveys subjected to statistical analysis, a conceptual framework was developed incorporating the empirical phases of the study as well the existing body of knowledge on the subject. This framework can then be used to enhance the creation, documentation and refinement of Information Security policy within the context of an ISMS implementation further supporting the embedment of discourse around information security discourse more precisely, but importantly, more inclusively.

In summary, the statistical analysis required for validity and objectivity of the study was catered for by tried and proven methods which were then compared against interview responses, where the questions (open ended) were carefully designed to elicit a response that pointed to the ineffectiveness or effectiveness of the policies in conveying the desired management and organisational intent. Thus, criterion validity was proved by comparing the statistical outcomes from the models with the narrative from respondents.

3.12 Ethical Considerations

To conduct research involving people, it was critical to ensure the researcher behaved ethically, and avoided misconduct, questionable research practices and that respondents or interview subjects were treated reasonably (Pimple, 2002). The researcher was granted ethical clearance to conduct the study by submitting the research questions and instruments for review. A letter to confirm ethical clearance was returned by the Universities' Ethics approval committee which can be found in Appendix 11.

All outcomes from the surveys have remained confidential without mentioning individuals or groups. Survey respondents were not contacted during or after the study except if reminders were required to increase the completion of said surveys. Survey questions did not require the population of any personal information or individually distinguishing characteristics.

Moreover, for all research respondents, informed consent was required in every individual case (Creswell, 2014). All respondents and interviewees then confirmed they were not forced to participate, and they understood the nature of the study, its intent, and any other relevant information about the researcher.

The transcripts and results from the interviews were included as appendices in the final research report and omitted any uniquely identifiable information or characteristics around systems, people, names of technology and other confidential data.

All participants in the study consented to participating in the study and that participation was optional. This took the form of a declaration for both the online study as well as the interview analysis. Within the interview study, any respondent's refusal to consent then resulted in the termination of the interview process with any result disregarded and omitted from the overall study result.

With respect to consent from the organisation to perform the study, this was obtained from the Information Security Policy discipline head however it has not included in this

document, given the name and contact details of the approver, but was used to seek ethical clearance for the study.

With respect to participant recruitment, the target study organisation made use of an enterprise management system where all staff in the organisation have profiles. The researcher was given access to a staff list that removed all other characteristics or personally identifiable information. Essentially, the file only contained a listing of all staff First Name, Last Name, and email address from which the sample was randomly selected.

Additionally, given the content of the file and the proprietary nature of an exhaustive list of all staff and their email addresses, it was not possible to share the file outside of the organisation due to the protection of personal information act (POPIA), since all employees are also clients of the bank and treated as such. Consequently, the selection of participants, the communication requesting them to participate, the emailing of the link to participate in the survey as well as the selection of the interview participants and the resultant interviews themselves were all conducted using organisational networks and infrastructure thereby ensuring data privacy and confidentiality.

3.13 Data Analysis

Since the research methods utilised within this study are varied (mixed-methods approach) and include surveys, the Cloze deletion method inclusive and interviews, detailed data analysis is required to ensure the validity and integrity of the research outcomes. This has involved both inferential and analytic methods. Much of the data collected is classified as categorical data, ordinal and nominal in nature, like education level for example which is classified as continuous and/or interval data. Some of the data for example, like period of employ in the organisation and age are continuous data.

To simplify the collection of some of the ordinal data, a Likert scale was used, and the data is presented in simple formats for analysis and explanation. This entails the use of descriptive analytic methods and frequencies to present the data in simplified tables, graphs, and charts. Descriptive analysis involved the inclusion of percentage summaries to provide answers to the research questions.

Moreover, the data provided is analysed statistically to ascribe inference or correlation which is considered inferential (Creswell, 2014). Conversely, descriptive analysis is used to derive relationships between more than one set of data that may not be evident from statistical analysis. This data is presented in tables, graphs, and figures with the objective to answer the research objectives. Consequently, to satisfy the nomothetic aims for this research, a combination of inferential and descriptive analysis was used to interrogate the study data. 45 interviews were conducted, and 46 completed questionnaires were analysed in total.

When inferential analysis is conducted, proven statistical methods are to be employed (Semenick, 1990) including the use of T-Tests which compares the sample mean to the population mean (Ruxton, 2006) and Univariate Analysis of Variance (ANOVA) which can interrogate a combination of independent and dependant variables (Kaufmann and Schering, 2007).

Cronbach's alpha, developed by Lee J. Cronbach in 1951, is a widely used statistical measure of reliability or internal consistency in research and psychometrics. It is designed to assess the extent to which a set of items or variables in a questionnaire or scale measure a single construct or domain consistently (Cronbach, 1951). Cronbach's alpha is a coefficient that quantifies the reliability of a measure by indicating the degree to which the items in a scale are interrelated and has several advantages. It allows researchers to evaluate the reliability of multi-item scales, determining the extent to which items are contributing to the overall consistency, and identify items that may need modification or removal (Devellis, 2016). In addition to this, Cronbach's alpha provides a simple and intuitive way to assess internal consistency. The use of Cronbach's alpha within the scope of this study has been to establish internal consistency of the quantitative instruments. In addition to this, Chi-square testing was used to analyse the associations between categorical variables and assess if the observed frequencies differ significantly from the expected frequencies (Agresti, 2002). It is a non-parametric test that is widely employed in various fields, including social sciences, healthcare, market research, and genetics. In addition, Chi-square tests do not rely on specific assumptions about the underlying distribution of the data, making them robust and applicable in situations where data may not meet parametric assumptions.

The use of Chi-square tests within the scope of this study was relevant due to the fact that Chi-square tests can be applied to different types of categorical data, including nominal and ordinal variables (Maroco and Garcia-Marques, 2013). They are therefore suitable for analysing data that can be grouped into categories or frequencies. Another advantage of the use of the Chi-square test within the context of this study, is its simplicity which outputs a Chi-square statistic and a p-value to indicate the level of significance. Finally, statistical analysis of the data involved the use of the one-sample t-test which is used to compare the mean of a single sample to a known or hypothesized population mean. It is a commonly employed inferential statistical technique to determine whether the sample mean significantly differs from the population mean (Bland and Altman, 1995).

The one-sample t-test is particularly useful in research settings where researchers want to examine whether a sample is representative of a larger population or if there are significant differences between the sample and the population mean. Its significance within the context of this study has been to assess whether the sample data provided sufficient evidence to reject or accept the null hypothesis (Rosner, 2015) and draw conclusions about the population mean and enable informed conclusions about the population and sample inferences.

SPSS or Statistical Package for Social Sciences is a software tool that enables researchers to conduct statistical and inferential analysis such as the calculation of Cronbach's alpha, Chi-square testing and one-sample T-test as well as ANOVA tests where the output is reliable (Bryman and Cramer, 2009) and was used to analyse results statistically.

Finally, it is important to define the methods used to combine all the data from disparate and unique sources to ultimately inform the research outcomes given the bias mentioned where it is possible to favour one data source over another in cases where the data from said sources may be contradictory or include many outliers (Bhandari, 2023). Data triangulation involves the use of different data sets by analysing the validity, influence and richness of data while also reducing the significant influence of a single source of data.

Data triangulation protocols were used within the interpretation and analysis stage of the research (in Chapter 4) and involved the interrogation of dissonance data as well as that

of convergence where data from each of the data sources were compared to understand if they complemented each other or differed. Since dissonance is not a problem in that it informs more reliable insights and outliers and may often provide material insights where mixed-methods is used (Wasti et al., 2022).

Two proven methods for data triangulation can be used (O'Cathain et al., 2010) which include a Mixed Methods Matrix – where all the data collected is combined pertaining to questions posed via the research (not survey questions) into a matrix view (Wendler, 2001) which for the purposes of this mixed methods approach was not feasible: the data from interviews collected was significant and could not be compared on a matrix with survey results.

The second method, called "Following a thread", was more suitable within the context of this study since it involves identifying significant themes and informing questions that must be answered via the data (Moran-Ellis et al., 2006) by following the thread thorough the different data sets. Given the overall views emanating via the surveys and obvious themes emanating from the questionnaires, following a thread was best suited to the data and was therefore used.

3.14 Data Quality

Ensuring reliable data collection methods is critical to informing a reliable research result. Data quality management in research involves utilising a validity instrument which is capable of measuring the efficacy of the instrument and expressing a reliability factor of overall research accuracy (Taan and Hajjar, 2018).

In terms of the reliability and validity of test results, it is important to note that the outcome from the SMOG, Fry and Cloze test are not inherently prone to errors as the calculations and application of the rubrics are designed to simplify outputs. Therefore, it is not anticipated that errors are a likely result. In terms of the surveys which were used as the "control" for the study, the researcher utilised a one-dimensional construct for assessing responses. This means that all questions posed to the research subjects within the interview setting sought to assess the respondent's ability to understand the policies directly as well as the intent.

To ensure adequate data quality for the Likert scale portion of the survey, statistical validity was required, where validation was enabled using various statistical and reference models detailed in Chapter 4.

3.15 Limitations

Limitations included the utilisation of linguistic study mechanisms against information technology policies which the researcher had no prior experience in conducting which required considerable learning and refinement to create reliable outcomes for the study. Further to this, the use of interviews presented the challenge in that even to closed questionnaire style interviews, respondents may respond a specific way, whether biased or otherwise purely due to the formal nature of the interview with the inherent fear that providing the wrong answers may carry some negative workplace repercussions. This could not be totally evaded, and the necessary assurances were provided to all respondents to allay fears.

In addition, the researcher was a full-time employee within the consenting organisation and thus limited time was available to conduct the study and all research and analysis had to be conducted after hours and on personal time to avoid any conflict of interest or repercussion of dereliction of duty.

Further, it must be noted that the researcher approached the South African Banking Risk Information Centre to facilitate discourse with all major South African banks to participate in this study, however, this proposal was rejected by the other banks given that the study would then expose their internal policies and procedures for information security to the researcher who is an employee at their competitor bank.

While the study was performed at one South African bank, it was not possible to extrapolate the results across the banking sector due to the differing nature, content, alignment, and communication mechanisms used for information security policies and procedures across the banks and financial services sector as a whole. However, as all banks in South Africa share similar characteristics, it is not inconceivable that they would benefit from the results of the study.

With respect to the interviews, it was originally anticipated that the volunteer rate may be low due to the one-on-one nature of interviews, but the researcher originally anticipated obtaining the required responses. The survey required 214 respondents (which represents 15% of the total sample population). This is a significant number of responses to receive given the limitations involved with the Cloze test where respondents must guess deleted words.

To complete the survey, participants received a link, which when clicked routed to the survey monkey website and the survey was opened automatically. It was not possible for respondents to leave a survey incomplete. Therefore, settings on the website forced that all fields were mandatory, which is the reason why there are no blank fields in the Cloze deletion test results. Further, if respondents closed the survey at any point or abandoned it at any point, not only were the incomplete results discarded by the site automatically, but the only way to then submit a response was to restart the survey from the beginning.

This mechanisms significantly improves the reliability and validity of the results in that respondents answering in a single sitting (Ardalan et al., 2007) more closely fulfilled the requirements of the Cloze deletion test, which is to guess-replace versus researching, calculating and "cheating" to guess the missing word. For the guessed word to match the deleted word, it had to be the exact deleted word and the researcher ignored misspelling. If the word deleted was a technical term/acronym or abbreviation, then only the exact match was deemed acceptable (Cheng and Warren, 1999). Synonyms were deemed acceptable and the tool was able to mark instances where synonyms were used versus the actual expected deleted word.

Most tools do not allow fill-in-the-blank surveys for multiple words in a sentence and therefore an important limitation was the ability for the Cloze test to be administered and for respondents to persist without abandoning completion before submitting.

3.16 Conclusion

This chapter has detailed the methods, strategies and data collection mechanisms used to inform the study. Data analysis and quality control concepts have also been described as

well as the methods to process quantitative data from surveys and the results from the Cloze deletion test. The following chapter will utilise the concepts and mechanisms in the preceding chapters to interrogate and interpret meaningful outcomes from the data collected.

CHAPTER 4

Analysis, Findings and interpretation

4.1 Introduction

This chapter presents all the data collected throughout the study including the Cloze Deletion Test (Surveys), interviews and the opinions contained therein as well as the results of the SMOG and Fry readability measures, to inform possible answers to the research questions and overall problem statement. This chapter details the descriptive and inferential results of the data collection process and how this data answers the research hypothesis.

The primary data collection instrument used were the survey which included 3 sections, Section one was the Biographical questions, section 2 the Likert scale questions about readability and awareness, and the third section, the Cloze deletion test.

The secondary data collection instrument used were the one-one-one interviews where readability, awareness and variables such as tone, language, workplace implications and improvement suggestions were analysed.

This section also includes subjecting the results from the test metrics to statistical scrutiny including Factor Analysis and other inferential and normalising tests.

Chapter 4 takes the following format:

1. Survey response rates are described and analysed for suitability within the context of the study and in line with the study objectives.
2. Demographic data is presented and analysed using graphs and tables to compare the data using descriptive analysis of the various charts and tables.
3. Data reliability imperatives are presented through the discussion and use of inferential statistics to confirm reliability via Cronbach's Alpha test as well as the use of the T-test to calculate the mean and its significance for each individual construct. Further to this Factor analysis was performed on the conceptual model

of the study to identify significant correlations as well as their strength and direction.

4. A question by question analysis for responses to Section 2 of the survey is then provided including relevant and characteristic outcomes.

5. The results from the Fry readability test, SMOG tests as well as the Cloze deletion test is then presented.

6. This is then formulated into an outcome comprising the quantitative section of the research findings. Since this was a mixed-methods study, the interviews were coded and themes emanating from the analysis are then presented.

7. The conceptual framework developed to answer the research aims and objectives is then expounded, presented, and discussed in the context of the empirical phases of the study.

4.2 Sample and response rate

A total of 46 responses (21,5%) were received out of a sample size of 214. The calculation of the sample size out of the total population involved the use of the formula created by Naing, Winn and Rusli (2006) where populations are finite. While the response rate was lower than anticipated (likely due to “survey fatigue” which occurs within the field of survey research and is indicated by a decrease in respondents’ willingness to participate or ability to provide accurate and thoughtful responses as a result of being exposed to a large number of surveys (Tourangeau et al., 2013), the "rule of thumb" of having a sample size of at least 30 participants is a general guideline often used in various research fields, but it is not specific to the Cloze deletion test. This guideline is based on the Central Limit Theorem, which states that the distribution of sample means approaches a normal distribution as the sample size increases, with 30 being a commonly cited threshold (Lumley, et al., 2002). Therefore, while not ideal, the sample is deemed adequate.

Eliciting survey responses involved an email to the respondents, randomly selected out of the total population requesting them to voluntarily participate in the study with a link to the survey site at www.surveymonkey.com. All surveys completed are considered valid for this study since all questions in the online questionnaire were marked as compulsory to be populated before the respondent could select “submit”, thereby committing their responses.

The low response rate of surveys is further attributed to the complexity involved in answering the deletion test and "survey fatigue". The average time taken to complete the survey was 30 mins, but it appears that most respondents started completing the biographical data and when prompted to complete the Cloze deletion test, populated a few guesses before giving up and abandoning the survey without completing it (this is indicated by survey analytics compiled by the online survey tool website) (these responses were discarded for completeness). Given the nature of fill in the blank tests especially where a respondent is asked to populate many blank fields, it is not uncommon for response rates to be low, especially where such tests are not compulsory. Moreover, given cognitive load theory (Sweller et al., 2011), where an individual's cognitive load is increased to generate multiple responses, the potential for mental exhaustion is increased and this results in a reduced motivation to finalise the task at hand. Further research has indicated that specifically in research instruments requiring extended responses, like fill-in-the-blank surveys, lower response rates are noted as they are perceived as more challenging and requiring greater cognitive load as compared to multiple choice questions (Zieky, 2001). It is however important that cognitive load requirements and perceived complexity are not the only possible impediments to fill-in-the-blank survey completion, and cannot be ruled out as well as potential reasons.

The survey itself (Appendix 2) was comprised of 3 sections. Namely, 1 – Demographic information such as gender, age, number of years of employment and education level. The second section collected data on a 5-point Likert scale about familiarity with the organisations Information Security policy, their implications on daily duties, accessibility, readability (ease of use), awareness, possible views around improvement, grammar, tone, language, and brevity as well as perceptions around training in the last 12 months. The third section comprised entirely of the Cloze deletion test with a 250-word passage from the Information Security policy surveyed with every 5^{th} word deleted and requiring the respondent to guess the missing 5^{th} word.

For the interviews, 45 remote interviews were conducted with another group of staff also randomly selected from the total population. The overall perspectives are presented according to themes emanating and overall trends. The interviews are largely opinion based and subjective based on various characteristics not limited to:

- Age
- Education level
- Total exposure to Information Security as a Discipline
- Pre-existing biases on the interviewee side
- Personality and characteristic traits
- Fear (many interviewees viewed the random selection as intentional management interventions aimed at assessing the employee's familiarity with information security as a practice. While every effort was made to inform employees that their participation was voluntary, random and their responses would not be shared with management, the possibility that employees saw the interview as a "test" cannot be excluded.

Therefore, it is not prudent to present individual perspectives from the interviews unless they are considered uncharacteristic or represent "fringe" views not in keeping with the opinions of the larger interview cohort. All interviews were recorded on Microsoft Teams which was the tool used to conduct the interviews remotely.

4.3. Demographic and background information of respondents

The aim of including biographic data questions was to include the possibility of identifying any significant relationships that existed between biographic data and the studies main constructs. The elicited responses to these questions are provided in Table 4.1 below:

Biographic Measure	**Data**	**Percentage**
1. Gender	Male	43.4
	Female	56.5
	Other	0
	Prefer not to say	0
2. Age	18 - 24 years old	0
	25 - 34 years old	30.4
	35 - 44 years old	52.1
	45 - 54 years old	15.2

	55 years old +	2.1
3. Period of employment at organisation	0 - 5 years	58.6
	6 - 10 years	21.7
	11 - 15 years	13.0
	16 - 20 years	4.3
	21 years +	2.1
4. Current education level	Primary school	0
	High school	8.6
	Undergraduate qualification	26.0
	Post graduate qualification	65.2

Table 1.1: Survey demographics

The one sample T-test was calculated for demographic data in order to analyse if the data collected contained any statistical inadequacies which would be an indicator of limited generalizability within the context of this study. Skewing of demographic data could potentially hinder the generalizability of results and further could create instances where confounding variables that are not properly controlled for, adversely affect overall generalizability as well (Maxwell et al., 2004). Moreover, given the aim of the study and underlying hypothesis, it was important to analyse all demographic groups within the study site to maximise the studies ability to be extrapolated to the total population. Moreover, subjecting the demographic data to statistical analysis provided reliable results to enable the assessment of whether a specific demographic variable differed significantly from a theoretical expectation (Babbie, 2016). Consequently, the one sample T-test was calculated on all demographic data sets to ensure that the sample data was statistically significant.

For all T-tests, where the t-value is small, this means that the difference between the sample mean and hypothesized mean is also small. The converse is true, larger t-values indicate larger differences. With P-values, the value itself indicates the probability of observing the obtained t-value under the null hypothesis, which therefore assumes that there is no significant difference between the sample mean and the hypothesized

population mean. As a result, a small p-value (usually less than 0.05) suggests that the observed difference is statistically significant and therefore the null hypothesis is therefore rejected (Babbie, 2016).

Demographic data indicates that the gender makeup of respondents was not equally comprised with 43.4% of respondents of the male gender and 56.5% of the female gender. No respondents selected “other” as gender and no respondents chose not to disclose their gender by selecting “prefer not to say”. The one sample T-test for respondents’ gender is statistically significant, p-value, t=-1196, p<.001.

The age of respondents was dispersed where no respondents indicated an age of between 18-24. 30.4% of respondents selected the age group 25-34. The largest group of respondents selected 35-44 years old, 52.1%. Lastly 1 (2.1%) respondent selected 55 years or older. The one sample T-test for respondents age is statistically significant, p-value, t=-801.4, p<.001.

In terms of years of employment at current organisation, the majority of respondents had been employed for the period 0-5 years and accounted for 58.6%. The second largest group of respondents had been employed for 6-10 years and accounted for 21.7%.

Long service employees (10 Years +) were comprised of 11-15 years totalling 13%, 16-20 years, 4.3% and 21 years or more at 2% respectively. The one sample T-test for respondents’ employment duration is statistically significant, p-value, t=-594, p<.001.

Where respondents’ education level is concerned, no respondents indicated a current education level of Primary school, with only 8.6% of respondents selecting a High school qualification. 26% of respondents indicated a level of Undergraduate, while the majority of 65.2% indicated an education level of Postgraduate qualification. The one sample T-test for respondents’ education level is statistically significant, p-value, t=-895, p<.001.

4.4 Reliability testing and statistical analysis

In order for reliable statistical outcomes to be created, an assessment of the research instruments efficacy is mandatory (Taber, 2017). Cronbach’s Alpha Test was conducted

on the study's variables to assess the surveys' reliability (Cronbach, 1951). Cronbach's alpha reliability test assesses the internal consistency to inform an adequate reliability scale for collected data where the minimum viable result is 0.60 (Tavakol and Dennick, 2011) and the values for Cronbach's alpha ranging between 0 and 1 with lower values indicating weaker or impaired contributions toward the measurement construct under analysis. Conversely, higher values point to questionnaire items that positively contribute toward the enquiry construct (Bujang et al., 2018). The result from this calculation present in Table 4.2 below which indicates a Cronbach's Alpha of 0,69 therefore indicates a value above minimum viability, (gender, age, period of employment and education level was removed from the calculation since it has no statistical bearing on the reliability data) (Wessa, 2021) and is thus considered acceptable and reliable.

Reliability Statistics	
Cronbach's Alpha	Number of Items
0,69	9

Table 4.2: Cronbach's Alpha Result

It must be noted that the Cloze test result was excluded from the calculation since it is a standalone research instrument and has its own reliability and validity constructs which have been detailed in Chapter 2.

Data normality also plays a crucial role in the estimation of confidence intervals and the calculation of p-values, which are essential components of hypothesis testing (Moore, McCabe, & Craig, 2012). When data are normally distributed, researchers can use the properties of the normal distribution to estimate the likelihood of observing a particular sample mean or test statistic under the null hypothesis. This information is then used to determine the statistical significance of the results and make decisions about whether to reject or retain the null hypothesis.

There are several advantages to assuming data normality in research. First, the normal distribution is mathematically tractable, making it easier to derive and apply statistical tests (Field, 2013). Second, the normal distribution is a good approximation for many

real-world phenomena, such as height, weight, and intelligence scores, making it a useful model for a wide range of research questions (Gravetter & Wallnau, 2016).

However, it is important to note that not all datasets are normally distributed, and researchers must assess the normality of their data before applying parametric tests. Various methods can be used to test for normality, including graphical techniques (e.g., histograms, Q-Q plots) and formal statistical tests (e.g., Kolmogorov-Smirnov, Shapiro-Wilk) (Field, 2013 and Gravetter and Wallnau, 2016).

The one-sample t-test is also useful because it is robust in its analysis violations of normality, especially in cases where sample sizes are large (Lumley, Diehr, Emerson, & Chen, 2002).

The one sample t-test requires only a single sample of data, making it more accessible and less resource intensive versus other statistical tests that require multiple samples or complex designs (Field, 2013) which are often not feasible.

This simplicity also extends to the interpretation of results, as the test produces a single t-value and associated p-value, which can be easily compared to a predetermined significance level (α) to determine if the null hypothesis should be rejected or retained. These ease of use and simplicity is why it was chosen for use in this study.

In order to internally validate all questions, the P values of each T-test is expressed. This was performed to test the potential for null hypothesis that the surveyed sample is the same as the populations mean.
There were 9 questions in the survey posed after the demographical questions, which were posed to gain insights as to opinions regarding accessibility, readability, comprehensibility, training compliance, simplification in language, and awareness success. These questions were completed by respondents using a 5-point Likert Scale.
These 9 questions were subject to Cronbach's alpha test, with the output indicated below:

While Cronbach's alpha test confirmed the questionnaire items contribution toward the measurement of the construct under inquiry (with a value of 0.69 >0.60 (minimum viable)), it was necessary to analyse associations between variables as well.

The Chi-square test for independence is the most suitable metric since it can establish the statistic relationship between two categorical variables (Plackett, 1983). This then allowed a calculation to establish if there was significant association between the respondent's education level (graduate or non-graduate) and their ability to read the document.

The formula for calculation is as follows:

$$\mathrm{X}^2 = \sum_{i=1}^{r} \sum_{j=1}^{c} \frac{(O_{i,j} - E_{i,j})^2}{E_{i,j}}.$$

The variables are as follows: for r rows and c columns of n observations, O is an observed frequency and E is an estimated expected frequency. The expected frequency for any item is estimated as the row total times the column total then divided by the grand total (n).

To perform the chi-square test, a contingency table was required with the counts of graduates and non-graduates who could and could not read the document indicated in Table 4.3. The null hypothesis (H0) was that there was no association between the respondent's education level and their ability to read the document. The alternative hypothesis (H1) was that there was an association between the two variables.

	Could read	Could not read
Graduates	42	0
Non-Graduates	0	4

Table 4.3: Contingency table

Using the contingency table, it was possible to calculate the chi-square test statistic (χ^2) and the corresponding p-value to determine if there was a significant association between the respondent's education level and their ability to read the document. An appropriate significance level (α) for the test, such as 0.05, to determine if the results were statistically significant.

It was then possible to calculate the chi-square test statistic (χ^2) using the formula:

$\chi^2 = \Sigma [(Observed\ count - Expected\ count)^2 / Expected\ count]$

Applying this formula to each cell, the following calculation was made:

$\chi^2 = (42-38.26)^2/38.26 + (0-3.74)^2/3.74 + (0-3.74)^2/3.74 + (4-0.26)^2/0.26$

$\chi^2 \approx .36 + 3.74 + 3.74 + 54.31$

$\chi^2 \approx 62.15$

Then it was necessary to determine the degrees of freedom (df) for the test. The formula for degrees of freedom is : *df = (Number of rows - 1) * (Number of columns - 1).* In this case, *df = (2 - 1 * (2 - 1) = 1.*

Finally, in order to compare the calculated chi-square test statistic (χ^2) to the critical value from the chi-square distribution table at the chosen significance level (α). The significance level chosen was $\alpha = 0.05$, the critical value for *df = 1 was 3.841.*

Since the calculated χ^2 *(62.15)* was greater than the value *(3.841),* the null hypothesis was rejected (H0) and it was therefore concluded that there was a significant association between the respondent's education level (graduate or non-graduate) and their ability to read the document.

4.5 Factor Analysis

Factor analysis is a statistical technique used to reduce a large number of variables into fewer numbers of factors. This technique extracts maximum common variance from all variables and puts them into a common score, which can be used for further analysis. Factor analysis is part of the general linear model (GLM) and assumes several conditions: a linear relationship, no multicollinearity, inclusion of relevant variables in the analysis, and a true correlation between variables and factors. Principal component analysis is one of the most commonly used methods in factor analysis (Kim et al., 1978).

Factor analysis is a useful tool for investigating variable relationships for complex concepts such as socioeconomic status, dietary patterns, or psychological scales. The key concept of factor analysis is that multiple observed variables have similar patterns of

responses because they are all associated with a latent variable (i.e., not directly measured) (Watkins, 2018).

There are two main types of factor analysis: Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA). EFA is used to identify the underlying structure of a set of variables without any prior assumptions and where the identification of latent factors that may be present in observed variables (Cudeck, 2000), while CFA is used to test a predefined factor structure based on theory or previous research.

4.5.1 Confirmatory Factor Analysis

For the purposes of this research, the observed variables constitute the questionnaire items, in which case, there are 9 variables (Question 5-13, since question 1-4 (1. Gender, 2. Age, 3. Period of employment at organisation and 4. Current education level are excluded)).

The aim of CFA is to analyse how precisely the questionnaire items measure the latent factors (Desmedt et al., 2022). The CFA was conducted R-language. R-language provides various packages (e.g., lavaan, sem) that facilitate conducting CFA. These packages offer functions specifically designed for model specification, estimation, and evaluation. The output from the analysis includes parameter estimates, fit indices, and other relevant statistics, which can be used to write up the results of the CFA.

Researchers can utilize R-language to specify the CFA model using a syntax-based approach, estimate the model parameters using appropriate estimation methods (e.g., maximum likelihood, weighted least squares), and evaluate model fit using built-in functions or custom scripts. R-language also provides options for visualizing the results, such as path diagrams or standardized estimates.

According to Brown (2015), there are 3 key components of Confirmatory Factor Analysis:

1. Model Specification: CFA involves first specifying the theoretical model, which includes the identification of latent constructs (factors) and their observed

indicators (variables). This model is represented by a series of hypothesized relationships between the factors and indicators, known as factor loadings.

2. Model Fit Indices: Assessing the goodness-of-fit (or acceptability) between the hypothesized model and the observed data is crucial in CFA. Various fit indices, such as the chi-square test, Comparative Fit Index (CFI), Tucker-Lewis Index (TLI), and Root Mean Square Error of Approximation (RMSEA), are used to evaluate model fit. These indices provide information about the degree to which the model fits the data and its suitability for use.
3. Reliability and Validity Assessments: CFA allows for examining the reliability and validity of the latent constructs. Reliability is assessed through the examination of internal consistency, measured by Cronbach's alpha or composite reliability. Validity can be evaluated through convergent validity (assessing the degree of association between indicators and their corresponding factor) and discriminant validity (ensuring factors are adequately distinct from each other).

Using R-language, the following parameter estimates were tabulated, in Table 4.4:

Classification	Value
Number of variables in the model	9
Number of observed variables	9
Number of unobserved variables	0
Exogenous Variables	9
Endogenous variables	0

Table 4.4: Parameter estimates for CFA

According to Beavers et al, (2013) suitable ranges are between 5 and 20 samples for each parameter estimate. The lower range from a sampling perspective is 45 (9*5) with the upper range at 180 (9*20). Consequently, while the sample size of 46 is low, it is deemed adequate for CFA. The disclaimer however, is that while the sample size is impaired, the possibility that inaccurate results as a limitation for the CFA calculations is acknowledged.

A key step in performing confirmatory factor analysis is the alignment of the conceptual model to the data from the study ultimately informing construct validity and providing an indication of "fit" (Saunders et al., 2018). Given the conceptual framework developed and detailed in Figure 2.2 the hypothesized fit is deemed as adequate. Further, as has been established in Table 4.1, The Cronbach value indicates that correlations are within the acceptable range and observed to be significant where the range >.5 and $p<0.05$).

Based on the study variables as well as parameter estimates, the confirmatory factor analysis (CFA) in lavaan was created using R-Language. The results were as follows:

1. Model Fit: The CFA model fit is assessed by comparing the user model to the baseline model. The chi-square test statistic for the user model is 66.768 with 10 degrees of freedom, resulting in a p-value of 0.06. The baseline model has a test statistic of 3876.345 with 17 degrees of freedom and a p-value of 0.0720. These results suggest that the user model fits the data better than the baseline model, although the fit is not statistically significant at the conventional significance level of 0.05.
2. Comparative Fit Indices: The comparative fit indices (CFI) and Tucker-Lewis Index (TLI) are measures of incremental fit improvement over the baseline model. The CFI value of 0.786 and TLI value of 0.677 indicate that the user model has a modest fit improvement compared to the baseline model.
3. Standardized Root Mean Square Residual (SRMR): The SRMR value of 0.037 represents the average difference between the observed and predicted covariance matrices. A lower SRMR indicates better model fit, suggesting a good fit in this case.
4. Factor Loadings: The factor loadings represent the strength and direction of the relationship between each latent variable (f1, f2, and f3) and their respective observed indicators (q05, q10, q13, q06, q07, q08, and q09). The loadings should be interpreted as standardized coefficients. For example, the loading of f1 on q05 is 0.513, indicating a positive relationship between f1 and q05. Similarly, negative loadings indicate an inverse relationship.
5. Correlations: The correlations between latent variables (f1, f2, and f3) can be inferred from the factor loadings. For example, f1 and f2 have loadings of 0.739

and 0.420, respectively, on f3. This suggests a positive correlation between f1 and f3, as well as f2 and f3.

6. Variances: The variances represent the amount of variance explained by each latent variable and observed indicators. The variance of f3 is 0.232, indicating that it explains a substantial portion of the total variance in the model. The variances of the observed indicators (q05, q10, q13, q06, q07, q08, and q09) can also be interpreted similarly.

The observed fit indicators arising out of figure 4.1 below are as follows:

Comparative Fit Index (CFI)	0.786
Tucker-Lewis Index (TLI)	0.677
RMSEA	0.294

Table 4.5: CFI, TLI and RMSEA Output

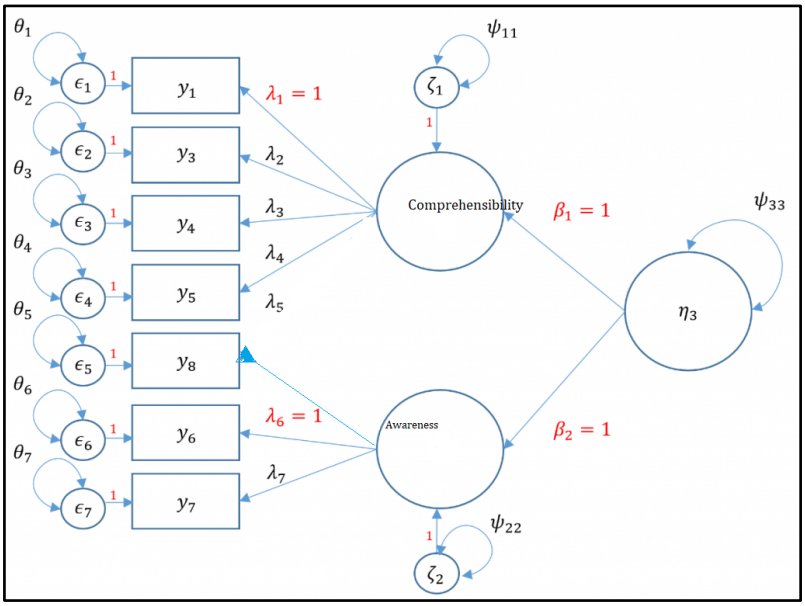

Figure 4.1: Confirmatory Factor Analysis of the Observed Variables

As can be seen in Figure 4.1, comprehensibility and awareness were latent factors that had an influence on how individuals responded to the Likert scale questionnaire data. Other variables that had an impact included those with language and comprehension which had the greatest influence on the outcome on the model and strategies made that incorporated communicating organization policies and information security. It was also hypothesized, that both awareness and comprehensibility in the analysis were depicted as influential. It was also assumed that comprehensibility of policies was correlated and thus influenced by some latent factor. From the output, the Tucker Lewis Index and the

Comparative Fit Index given suggest that the model is a “good” fit to the data. Additionally, there was no significant difference between the hypothesized model and the output of the data and are therefore the model is considered valid and reliable.

4.6 Inferential analysis

According to Pallant (2016), statistical inference is the analysis of sample data in relation to the total population. The aim being to understand whether or not the data collected is completely random or if it has a reliable and calculable probability of being inferential to the study’s population.

Within this study, inferential analysis includes various analyses and tests such as normality tests, which is a critical assumption in many inferential analyses, as it allows for the use of parametric tests that rely on the assumption of a normal distributions in data. Further to this, frequency distributions provide a descriptive summary of the distribution of values within data. They display the number of observations falling into various categories. An analysis of frequency distributions allows insights into the average, central tendency, and patterns within the data, which can guide subsequent inferential analyses (Stevens, 2012).

4.6.1 Normality testing

The assumption of normality is often crucial for accurate inference and hypothesis testing. The normality assumption states that the data or variables under investigation are distributed according to a normal or typical distribution (bell-shaped) with usually an equal number of measurements possible both below and above the mean value.

Parametric statistical tests, such as the t-test or analysis of variance (ANOVA), are designed for use with data that follow a normal or typical distribution. These tests rely on assumptions about the underlying population distribution, including normality. In situations where the population is viewed as atypical or not bell-shaped, it is essential to then use non-parametric tests for normality (Saunders et al., 2009). Using these in the incorrect configuration results in misleading or inaccurate results where normality is assumed inaccurately or without calculation.

4.6.2 Frequency distributions

For the 9 questions respondents were asked to answer in Section 2 of the survey, the following spread of responses is noted, in Table 4.6:

Question	Likert scale	Coding	Percentage
5. Are you familiar with the organisation's Information Security Policy and the updates made on an ongoing basis?	Yes	1	45,6
	Somewhat	2	50
	Unsure	3	2.17
	Not really	4	2.17
	No	5	0
6. Do you understand the implications of the policies on the daily performance of your work/tasks?	Yes	1	73.9
	Somewhat	2	21.7
	Unsure	3	4.3
	Not really	4	0
	No	5	0
7. Are the organisations information security policies easily accessible?	Yes	1	43.4
	Somewhat	2	41.3
	Unsure	3	6.5
	Not really	4	4.3
	No	5	4.3
8. Are the information security policies easy to read and understand?	Yes	1	56.5
	Somewhat	2	28.2
	Unsure	3	4.3
	Not really	4	4.3
	No	5	6.5
9. Do you believe there is adequate awareness around the information security policies within the organisation?	Yes	1	34.7
	Somewhat	2	45.6
	Unsure	3	4.3
	Not really	4	13
	No	5	2.1
	Yes	1	41.3

Question	Likert scale	Coding	Percentage
10. Are there are better ways for the organisation to communicate IT Security policies and the implications for you as an employee?	Somewhat	2	36.9
	Unsure	3	8.6
	Not really	4	10.8
	No	5	2.1
11. Is the overall language and grammar used within the IT security policies clear and concise?	Yes	1	50
	Somewhat	2	30.4
	Unsure	3	6.5
	Not really	4	8.6
	No	5	4.3
12. Do you think the policy authors have done enough to avoid confusing acronyms and abbreviations used in Information Security Policies?	Yes	1	28.2
	Somewhat	2	41.3
	Unsure	3	17.3
	Not really	4	6.5
	No	5	6.5
13. Have you attended any information security training, awareness or courses in the last 12 months?	Yes	1	82.6
	Somewhat	2	4.3
	Unsure	3	2.1
	Not really	4	2.1
	No	5	8.6

Table 4.6: Section 2 - Likert Scale Summary

The resultant frequency distribution summary from the Likert scale responses is contained within the Table 4.7 below:

		Question 5	Question 6	Question 7	Question 8	Question 9	Question 10	Question 11	Question 12	Question 13
		Are you familiar with the organisation's Information Security Policy and the updates made on an ongoing basis?	Do you understand the implications of the policies on the daily performance of your work/tasks?	Are the organisations information security policies easily accessible?	Are the information security policies easy to read and understand?	Do you believe there is adequate awareness around the information security policies within the organisation?	Are there are better ways for the organisation to communicate IT Security policies and the implications for you as an employee?	Is the overall language and grammar used within the IT security policies clear and concise?	Do you think the policy authors have done enough to avoid confusing acronyms and abbreviations used in Information Security Policies?	Have you attended any information security training, awareness or courses in the last 12 months?
N.	Valid	46	46	46	46	46	46	46	46	46
	Missing	0	0	0	0	0	0	0	0	0
	Mean	1,609	1,304	1,848	1,761	2,022	1,957	1,870	2,217	1,500
	Median	2	1	2	1	2	2	1,5	2	1
	Mode	2	1	1	1	2	1	1	2	1
	Standard Dev	0,649	0,553	1,032	1,158	1,064	1,074	1,147	1,134	1,225

Table 4.7: Section 2 – Frequency distribution

As can be seen in the table, the mean response is in excess of 1 (*M>1*), additionally, the median value is 1 or greater than 1 in all cases (*Mdn>=1*). In order to calculate whether the mean and median values are a reliable measure of central tendency, the one-sample t-test was used. This is because the assumption of normality can be violated without affecting the validity of the test (Wilcox, 2009). The theoretical midpoint of a 5 point Likert scale is 3, since this is often the neutral point where respondents are neither agreeing nor disagreeing with the statements/questions. Analysis of the responses indicates that there was no significant skewing of the distribution. This means that for the most part, across the survey questions responses were adequately distributed across the Likert scale. Therefore it was not necessary to use an empirical (where responses lean toward the positive end of the scale) or contextually derived neutral value. Within the context of this study, the null hypothesis is that the parametric (mean) is equal to a hypothesized neutral value of 3 (H_O: *M=1*) and the non-parametric (median) is equal to a hypothesized neutral value of 3 (H_O: *Mdn=3*). Moreover, as is evident, in each of the cases, the alternative hypothesis is that these measures of central tendency are significantly different from 1 ($\underline{H_a \neq 1}$).

Since the p-value was < α (0.05), the null hypothesis is rejected, indicating a statistically significant result since the confidence level was 95%.

4.7 Survey descriptive analysis

For question 5 which asked whether respondents were familiar with the organisation's Information Security Policy and the updates made on an ongoing basis that 50% agreed somewhat but still had potential issues which may not have inclined them to answer in the definitive "Yes". Notwithstanding, 45.6% of respondents confirmed that they were familiar with the Information Security Policy. 2.1% of respondents were unsure and 2.1% selected "not really" indicating that they au fait with the policy. No respondents selected "No". It is therefore clear from the survey that all employees are not familiar with the policy and in contrast no employees were unfamiliar at all. Since the policy applies to all staff within the employ of the organisation, it is possible that more can be done to socialise the policy and its content with staff. The results of the one-sample t-test revealed a statistically significant difference ($t = 923$, $p < .001$) between the sample mean and the specified value for familiarity with the organisation's Information Security Policy. With a significance level of $\alpha = 0.05$, we reject the null hypothesis and conclude that there is strong evidence to suggest that the sample mean significantly differs from the specified value.

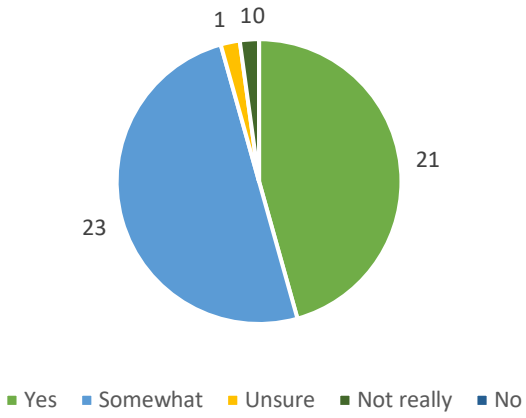

Figure 4.2: Survey Question 5

When asked if employees understood the implications of the policy on their daily tasks and duties, a majority of 73.9% indicated that they understood, with 21.7% indicating that the implications were understood, although not fully. Only 4.3% were unsure of the implications as it related to them daily. No respondents selected "No" or were "Unsure". Therefore, the analysis can determine that the majority of staff understand the implications, although potentially not entirely. Since the implications of the policy and information security as a whole are applicable to all employees with 4.3% indicating uncertainty not all employees understand the implications. The results of the one-sample

t-test revealed a statistically significant difference ($t = 1088$, $p < .001$) between the sample mean and the specified value for confirmation of understanding of policy implications on daily performance of work/tasks. With a significance level of $\alpha = 0.05$, we reject the null hypothesis and conclude that there is strong evidence to suggest that the sample mean significantly differs from the specified value.

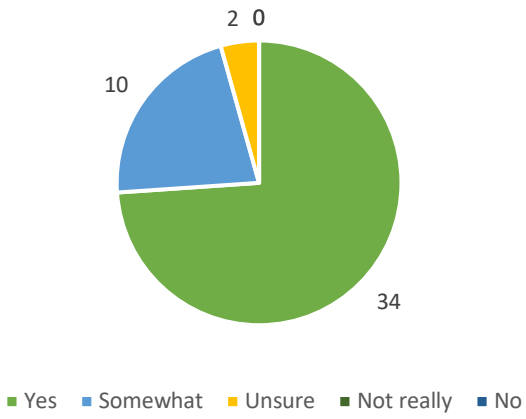

Figure 4.3: Survey Question 6

For question 7 which asked whether the organisations information security policies were easily accessible, 43.4% responded in the affirmative, with 41.3% responding that the policy was somewhat accessible but not entirely easily. 6.5% indicated that they were unsure whether or not the policy was accessible or not. Of all respondents, 4.3% responded that the policy was not easily accessible and 4.3% responded that the policy was not really easily accessible or indicating challenges. Therefore, 8.6% of respondents have indicated that the policy is not easily accessible. Since policy accessibility is critical, it is vital that ISMS implementors ensure ease of access and test same on an ongoing basis to confirm. The results of the one-sample t-test revealed a statistically significant difference ($t = 579$, $p < .001$) between the sample mean and the specified value for whether the organisations information security policies were easily accessible. With a significance level of $\alpha = 0.05$, we reject the null hypothesis and conclude that there is strong evidence to suggest that the sample mean significantly differs from the specified value.

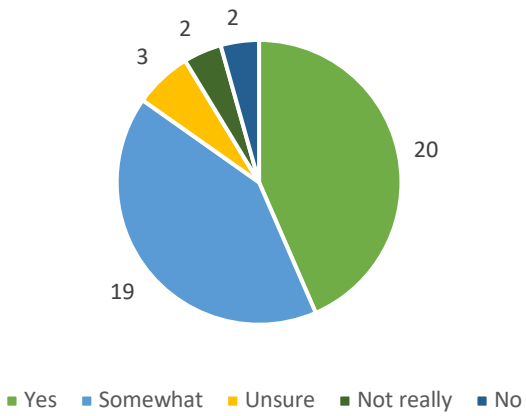

Figure 4.4: Survey Question 7

When asked whether the information security policy was easy to read and understand, the majority of respondents answered "yes" at 56.5%, with 28.2% saying the policy was somewhat easy to read and understand or that they had experienced challenges or issues. 4.3% indicated that they were unsure whether or not the policies were easy to simple. 4.3% responded "not really", or that they were not convinced around the policy's ease of reading and comprehension, with 6.5% confirming categorically that they did not see the policy as easy to read and understand. If policies are not easy to read and understand, employees will not adhere to them. The results of the one-sample t-test revealed a statistically significant difference ($t = 516$ $p < .001$) between the sample mean and the specified value for whether the information security policy was easy to read and understand. With a significance level of $\alpha = 0.05$, we reject the null hypothesis and conclude that there is strong evidence to suggest that the sample mean significantly differs from the specified value.

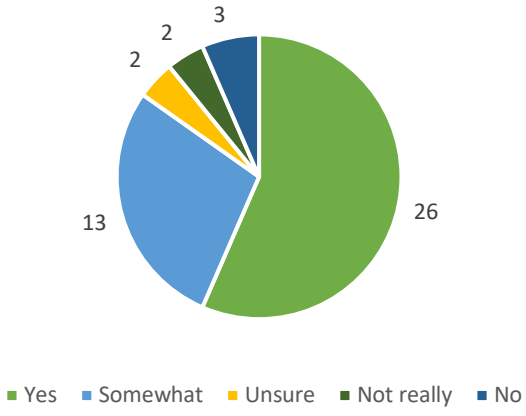

Figure 4.5: Survey Question 8

In terms of awareness, respondents were asked whether they believed that there is adequate awareness around the information security policy within the organisation. 34.7% of respondents confirmed their belief that there was adequate awareness. 45.6% responded that while there was adequate awareness there were issues which prevented them from selecting a Yes, emphatically. 4.3% were unsure. There were 13% of respondents who indicated that awareness was not really adequate and 2.1% who selected a direct No regarding adequate awareness. The results of the one-sample t-test revealed a statistically significant difference ($t = 560$ $p < .001$) between the sample mean and the specified value for whether there was adequate awareness around the information security policy within the organisation. With a significance level of $\alpha = 0.05$, we reject the null hypothesis and conclude that there is strong evidence to suggest that the sample mean significantly differs from the specified value.

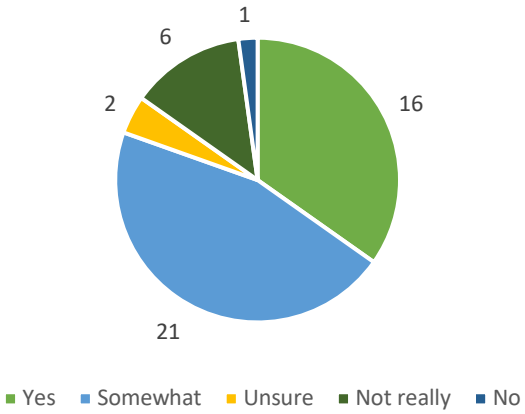

Figure 4.6: Survey Question 9

Respondents were also asked whether there were better ways for the organisation to communicate IT Security policy better including the implications of said policy to employees. 41.3% responded “Yes” indicating that they believed there were better ways for the organisation to better communicate policy implications to employees. 36.9% indicated “somewhat”, which can be interpreted to mean that they did think there were better ways to communicate but were not entirely sure what those ways might be. 8.6% of respondents were unsure, with 10.8% responding “not really”, or that they were overall comfortable with the currently used ways of communicating policy implications to employees. Only 2.1% responded “No”, or that they did not believe there were better ways for the organisation to communicate policy implications better. The results of the

one-sample t-test revealed a statistically significant difference (t = 556 p < .001) between the sample mean and the specified value for whether respondents believed there were better ways for the organisation to communicate security policy implications to staff. With a significance level of α = 0.05, we reject the null hypothesis and conclude that there is strong evidence to suggest that the sample mean significantly differs from the specified value.

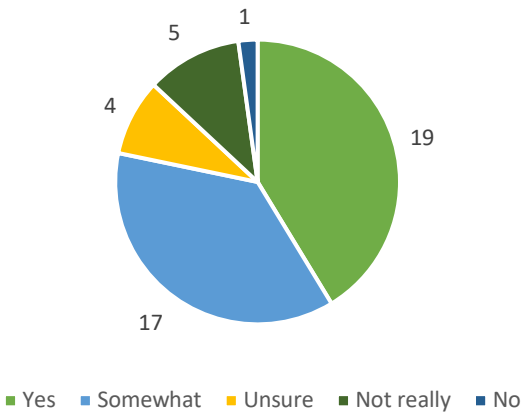

Figure 4.7: Survey Question 10

For question 11, respondents were asked whether the overall language and grammar used within the IT security policy was clear and concise. 50% of respondents "yes", or that they viewed the language and grammar as clear and concise. There were 30.4% of respondents who indicated "somewhat", or that while the grammar and language was overall clear and concise, it was entirely not so. 6.5% of respondents were unsure. There were 8.6% of respondents who indicated that overall language and grammar was "not really" clear and concise or that overall, the policy language was problematic, with 4.3% selecting "no" and confirming that in their view there was no clarity and conciseness in the overall language and grammar used within the policy. The results of the one-sample t-test revealed a statistically significant difference (t = 521 p < .001) between the sample mean and the specified value for whether respondents believed that the overall language and grammar used within the policy was clear and concise. With a significance level of α = 0.05, we reject the null hypothesis and conclude that there is strong evidence to suggest that the sample mean significantly differs from the specified value.

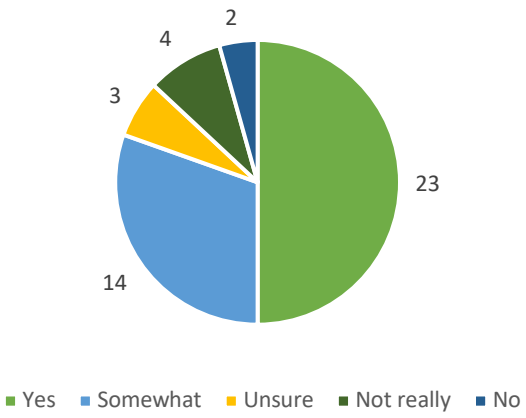

Figure 4.8: Survey Question 11

When asked if respondents thought the policy authors had done enough to avoid confusing acronyms and abbreviations used in Information Security Policies, 28.2% of respondents responded "yes". There were 41.3% of respondents who selected "somewhat" or that while they believed policy authors had attempted to avoid confusing abbreviations and acronyms, they had not entirely done so. There were 17.3% of respondents who were unsure. 6.5% responded "not really" or that they did not think policy authors had done enough entirely and 6.5% who outright selected "No", or that they did not believe at all the policy authors had done enough to avoid confusing acronyms and abbreviations. The results of the one-sample t-test revealed a statistically significant difference ($t = 525$ $p < .001$) between the sample mean and the specified value for whether or not respondents believed that policy authors had done enough to avoid confusing abbreviations and acronyms in the information security policy. With a significance level of $\alpha = 0.05$, we reject the null hypothesis and conclude that there is strong evidence to suggest that the sample mean significantly differs from the specified value.

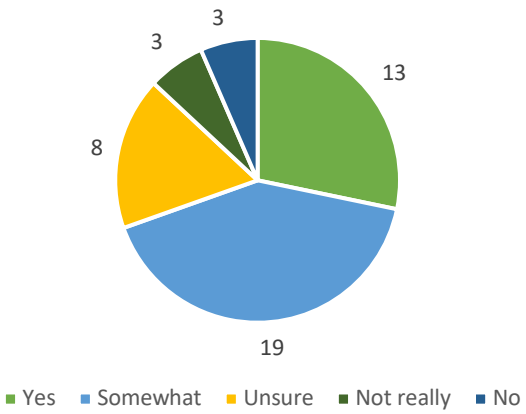

Figure 4.9: Survey Question 12

Finally, for this section of the survey, respondents were asked whether they had attended any information security training or awareness courses in the last 12 months. The overwhelming majority of respondents selected "Yes", indicating that they had attended awareness training or courses related to information security in the last 12 months. "Somewhat" was selected by 4.3% indicating that they had attended training and or awareness courses in the last 12 months but were not really sure. 2.1% selected "unsure". 2.1% of respondents responded "not really" or that they did not think they had attended any training or awareness courses and 8.6% responded with a "No" that they did not attend any information security courses or training pertaining to information security in the last 12 months. It is important to note that the organisation provides information security training on an ongoing basis and all employees. Contractors and 3rd parties are automatically enrolled for information security training whenever new content/courses are made available. This training is mandatory. The results of the one-sample t-test revealed a statistically significant difference ($t = 490$ $p < .001$) between the sample mean and the specified value for whether respondents had attended any information security training, awareness or courses in the last 12 months. With a significance level of $\alpha = 0.05$, we reject the null hypothesis and conclude that there is strong evidence to suggest that the sample mean significantly differs from the specified value.

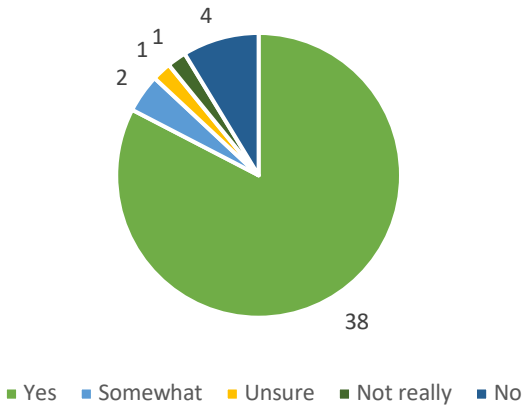

Figure 4.10: Survey Question 13

4.8 Frys readability

In order to calculate the Fry readability score, a 638-word extract was used in the Readability formula tool available at https://readabilityformulas.com/free-fry-graph-test.php. The sampled text included the introduction (143 words), the full policy extract for access control (231 words) and a 264-word extract for Mobile and Teleworking Security. This extract is presented in Appendix 3. A sufficient sample size is considered to be 3-4 (100 word) sentences and approximately 300-500 words in total up to a maximum of 2000 words.

Based on the extract in Appendix 3, the average number of syllables per word is 2 with total syllables in the text calculated at 1126. The total number of words with double syllables is 127 and the average number of words per sentence is 22.

The tool plots average number of syllables per 100 words which was calculated at 200 on the X-axis and plots the Average number of sentences per 100 words which was calculated at 4.6 on the Y-axis. Due to the tool's ability to only plot to a maximum of 172 average number of syllables per 100 words, the tool could not plot the X-axis on the graph (the red star indicates the convergence of the two points and as can be seen on the X-axis, the star is off the chart). A full analysis of the text is provided in Appendix 4, while the resultant Fry Readability graph is shown below in Figure 4.11:

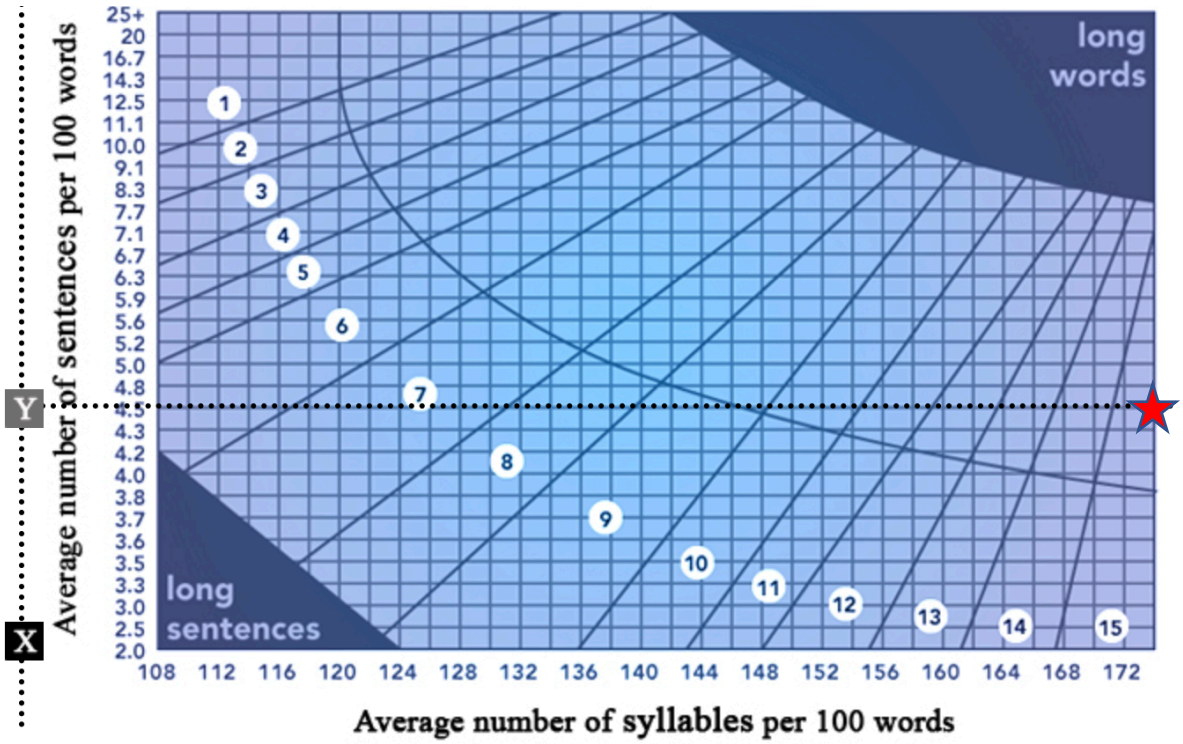

Figure 4.11: Fry's readability graph – Information Security policy

Given the high number of syllables per 100 words at over 200 (where the graph maximum calculation is 172), the readability of the text is calculated to be "Very difficult to read". Most respondents indicated undergraduate (26%) and postgraduate education (65%) levels but a classification of "very difficult to read" places the minimum readers capability at "university graduate level". According to Sibanda (2014), The South African result will be one level behind, i.e. "post graduate level". This is inadequate since it then excludes any reader with a reading level below that of a university post-graduate (8.69%) as well as undergraduates, 26%. This does however mean, according to the output that the document was deemed as readable by 65.2% of respondents.

The Information Security policy is applicable to all employees given its own scope indicated in the policy itself, "This policy applies to all employees of the organisation, as well as contractors and third parties and their employees." The assumption being that all those who indicated they were post graduates could read the document, and all those who indicated education levels below that of graduates could not read the document, it was necessary to establish the statistical significance and challenge this assumption.

Policies intended for consumption by all employees must be written at a level suitable for all employees. Given the Fry's readability outcome, the Information Security Policy is not written at a level for all employees across the organisation.

4.9 SMOG index

The use of the SMOG index involves counting 10 sentences in a row at the beginning, middle and end of the text (in this case the Information Security Policy) for a total of 30 sentences. Counting every word with three or more syllables in each group of sentences even if the same word appears more than once yields a total which is then square rooted and 3 added to the result. This provides the SMOG Grade. For this SMOG test, 30 sentences (Appendix 5) were used, and the result calculated according to the formula 1.0430 × square root (total polysyllables × (30 ÷ total sentences)) + 3.1291. This yielded a result of 16.59 on the SMOG Readability Index below in Table 4.8 and is indicated by a box border (Derguech, Zainab and D'Aquin, 2018):

Score	Education Level
4.9 or lower	Elementary school
5 - 8.9	Middle school
9 – 12.9	High school
13 – 16.9	Undergraduate
17 or higher	Postgraduate

Table 4.8: SMOG Readability Index Output

This means that the reading level of the 30 selected sentences is categorised as "difficult to read". This means that staff with a university qualification or a "graduate" were deemed as a minimum education level required to read the document. As the Chi-square test calculated a result indicating a statistically significant relationship between education level and reading or being unable to read the document, the outcome shows that the document could not be read by all staff, even though, by its own applicability clause, it was designed for all staff consumption. Therefore the result obtained via the Fry's readability calculator is corroborated by the SMOG Index result.

A 9% rate of readers being unable to understand the policy indicates that there is room for improvement. It is essential to gather feedback from those who had difficulty understanding the policy and identify the specific areas that caused confusion. This feedback can be used to revise the policy, making it more accessible and comprehensible to a broader audience.

In addition to revising the policy, the organisation can also provide training and support to help employees better understand the information security policy. This can include workshops, seminars, or one-on-one sessions to address any questions or concerns employees may have.

In summary, while a 9% rate of readers being unable to read the information security policy is not ideal, it is an opportunity for the organization to improve the policy's clarity and provide additional support to ensure that all employees can understand and adhere to the policy. Moreover, the percent of 3+ syllables is 24% with a total of 164 words (Appendix 6) with 3 or more syllables. “Polysyllabic” words are deemed as difficult to read. This means that according to the SMOG index, the policy can be categorised as unsuitable for all employees’ reading level.

4.10 Cloze deletion test

The Cloze deletion test involved respondents guessing every 5th deleted word from a 250-word passage from the Information Policy. This test involves assessing the predictability and repeatability of grammar, context, and tone in a document. Where a high percentage of correct words are guessed verbatim, the text is deemed to represent a high level of underlying inferred context and vocabulary. The converse is also true where a low correlation between the deleted words and guessed words represents a low level of inferred context and vocabulary. The underlying premise being that if respondents are able to accurately guess the missing/deleted words they are then more likely to grasp the context and intent of the text, and in this case, the information security policy.

Since the Cloze test was included in the survey, there were 46 responses. The sample passage (Appendix 7) was selected at the beginning of the policy in order to exclude too many acronyms and technical terms found throughout the document. Cued blanks were

not used, i.e., the length of the deleted word was not indicated by longer or shorter blanks. Although respondents were told to only substitute one word for each deleted word, there were instances where this was not performed, and more than one word was substituted. The full detail for each deleted word and the 46 guesses per word is provided in Appendix 9, including the percentage scored where guesses were correct. Words highlighted in green text indicate spelling errors or substitutions which are correct.

None of the deleted words were accurately guessed by every one of the 46 participants. There was one acronym which was included in scope as a deleted word as it was the fifth word, ISMS (Word 26) (Information Security Management System). This was only guessed correctly by 7 participants accounting for 15.2% of responses.

The most accurately guessed word, the preposition “is” (Word 44) was guessed correctly by 42 out of 46 participants, indicating a successful guess rate of 91.3%. The least successfully guessed word was ISMS.

18 words out of 55 were guessed correctly more than 50% of the time by respondents, while 7 words were guessed correctly less than 20% of the time.

Overall, the guess rate remained suboptimal and therefore from a Cloze deletion test measurement, respondents were unable to successfully guess the majority of words most of the time. Therefore, through inference, the chosen passage is considered complex and lacks a high inherent comprehensibility. This means that readers are unable to infer the content in the policy. Consequently, they may be unable to understand the intent, rendering the policy questionable from an effectiveness point of view.

4.11 Interview Results

45 interviews were conducted virtually via Microsoft Teams. Respondents were randomly chosen, and all respondents agreed to participate. All respondents were informed before the interview commenced that their participation was voluntary, no personal information was collected and that participants could stop the interview at any time. The transcription of all 45 interviews is provided in Appendix 10.

The following questions were asked to the interviewees:

1. Could you briefly describe IT Security to me?
2. What role does IT Security policy play in keeping an organisation safe from threats?
3. Do you believe our organisational IT security policies are adequate?
4. The use of jargon and technical terms is common in such policies, how should they be improved or simplified?
5. If IT security awareness specifically could be improved, what would that entail in your opinion?
6. In your opinion, are there adequate opportunities available to you to shape our IT Security programme or for your input to be incorporated?
7. Where would you locate our Information Security policy?

In order to simplify the presentation of outcomes from the interviews, the results, themes and ideas and any pertinent information are presented on a question-by-question basis in the following section:

4.11.1 Could you briefly describe IT Security to me?

In response to this question, there were varying views on information security. Many of the respondents aligned their understanding to their current roles and mentioned that information security is primarily concerned with protecting client's information from unauthorised access, or from parties seeking to obtain such information through unauthorised means.

The protection of personal information act (POPIA) was topical with many interviewees responding that information security was a consequence of the organisation's obligations in terms of POPIA. Interviewees who tended to have roles which were client facing tended to view information security as pertaining to ultimately protecting and securing information that the organisation may hold/process for and on behalf of the client through the existing contractual relationship, while employees who had internal focussed roles viewed information security more abstractly as protecting the organisation from threats

both internal and external, segregating access internally and in general mitigating or reducing the likelihood of cyber related threats.

From the responses to this question there was also a contingent of interviewees who had romanticised views around information security and spoke about hacking, cyber-fraud, ransomware, firewalls, spam reduction, phishing attacks, and mobile device security. These sentiments are best captured by the response “IT security is about safety within the company like VPN. I need to if I'm working from home I need to log in through VPN to make sure that the information of the company is not exposed to the wrong devices or the wrong people”, as well as “ OK, so for me IT security would be mitigating risk for like potential fraud, which is cyber related and making sure that the systems that we use are secured in order to protect information of clients as well as internal parties as well”.
There are many reasons for these views which can be attributed to social media, television, and the sharp rise in cyber-attacks on large corporates.

Interviewees also mentioned securing systems internally from other staff who may try to access. The underlying commonality in responses pertained to making sure information was kept secure and confidential, and that this information was not leaked intentionally externally or internally intentionally or accidentally. There were also responses around processing information securely which indicates a sense of the externalisation of data via vendors and 3rd parties legitimately which could pose risk.

Some respondents mentioned the securing of digital devices and platform protection while one interviewee mentioned “Mitigating risk for fraud which is cyber-related and protect information of clients and internal parties”.

Based on responses provided for this question the conclusion that can be drawn is that overall employees tend to understand information security concepts and its purpose in the organisation, how information security protects data and how underlying technologies might be leveraged in the organisational context to prevent theft, fraud and reputational impact resulting in financial loss to the organisation even if the respondents tended to, in some cases only understand it as it pertained to their specific role. This is not uncommon in an organisational context since some employees might have greater exposure to information security staff and related contexts primarily because of the specific role.

It was clear through the responses to this question that information security is important, and all organisations must communicate how important the discipline is with all staff.

Overall, responses did cover the core principles as outlined in the policy which are Confidentiality, Integrity and Availability of data and while not evident in absolutely all responses, these principles were discussed in many.

4.11.2 What role does IT Security policy play in keeping an organisation safe from threats?

Once again with this question, interviewees tended to focus on their understanding of information security based on the context of their specific roles versus viewing the policy holistically in an organisational context.

Very few of the interviewees mentioned governance, frameworks, or principles in their responses. While POPI was once against mentioned, there were no views provided which underlined the importance of security policy in terms of overall risk management and security.

Most, if not all agreed as to the importance while not all understood the implications of the policy in keeping an organisation safe from threats apart from stating widely that policy would serve to indicate what can be done to protect information from those with malicious intent.

One interviewee mentioned that it would “Guides the IT people and staff on how we can protect the information online”. There was heavy focus from a policy perspective around cyber related implications while one staff member mentioned “The policy basically is in place for my understanding to assist all banking staff to understand what measurements IT can put in place to make sure that they safeguard us from either going against banking regulation because the bank is also regulated by regulatory boards”.

In terms of regulation itself, there was no mention of ISO standards or other frameworks such as King code for corporate governance, COBIT (Control Objectives for IT), ITIL

(Information Technology Infrastructure Library) or COSO (Committee of Sponsoring Organisations) frameworks.

Many employees' perceptions around information security policy itself related to awareness initiatives and training. It is possible that this is as a consequence of the many trainings online training courses the organisation mandates for all staff where policy is referenced including but not limited to compliance, and repercussions for breaches or non-adherence to said policies/industry regulation.

Similar to question 1, various technology solutions were mentioned such as VPN, firewalls and antivirus. This was an unexpected result given the fact that the policy does include under its communication security section a number of principles around connectivity, intrusion detection systems, remote access and vulnerability management.

Overall responses to this question were varied and there were no strong common opinions provided which singled out governance or frameworks, but interviewees tended to understand the outcomes expected from the information security while not explicitly stating such.

The best summary of this intent was provided by one interviewee who stated, "Protect privacy and protect all information resources".

4.11.3 Do you believe our organisational IT security policies are adequate?

The overwhelming response to this question was "Yes" and while many reasons were provided most interviewees were comfortable only to provide a finite answer.

Some qualified their answer by stating that they believed the Information security policy was adequate because it was updated on a regular basis and took into account new threats and hacks which were newsworthy or publicised. Potential ways to improve the policy were inadvertently mentioned here as well including agility in policy-setting and increased awareness.

One interviewee did not believe the policy was adequate stating that there was not enough focus on governance and approvals as well as socialisation of the policy with staff. While adequacy and communication adequacy are two different things, it is still an important aspect to be factored in holistically in light of the question posed.

A largely characteristic view presented overall by interviewees is reflected by one answer, "Right. So mostly I would like to include what we call the cyber security whereby it is very important that the IT security protects all of those in terms of the boundaries on but ever that may affect the system of the company to threats from outside of people or cyber. That are trying to like try to maybe access the system of the company and in terms of maybe theft or whatever the case may be, that can be a danger to the business and to our clients as well." This quote summarizes quite well the underlying belief that IT Security policies are inherently adequate trusting that specialists formulate them, manage them, and communicate the necessary aspects to other staff within the organisation.

Another interviewee went so far as to say the policy was deemed adequate since there were no instances published or "floating around" which would be called "scandalous" or cause the information security of the organisation to be deemed inadequate.

From 45 interviewees, only one interviewee responded that they were not familiar with the policies and so therefore could not answer the question, while 2 interviewees responded with "No". Therefore, the implied consensus is that the policy is adequate, even though the question did not stipulate what adequacy would entail and left the challenge to the interviewee to decide what they considered adequate from this context.

4.11.4 The use of jargon and technical terms is common in such policies, how should they be improved or simplified?

The phrase used most repeatedly in across responses was "laymen's' terms". The majority view was that the simplest method to simplify jargon and technical terms was to use laymen's' terms or what is widely considered to be basic or simple language.

Therefore, the overwhelming view was that policies intended for all staff should remove acronyms, abbreviations, and jargon altogether and the policy should be written in simple

language with the purpose of being understood by all. A handful of interviewees shared views around policy writers knowing the readers were diverse and potentially would not understand jargon and technical terms and held the view that technical terms and jargon were specifically included to make the policy complex difficult, therefore making it more technical/specialised in nature. This could best be reflected by the response "Oh my word it's the same like when a client calls into stockbroking and they ask us about corporate actions, and they cannot understand. So, I would think that if they were jargon that was used, you know there's always synonyms that one can use when you use a specific. A specific word and it might not resonate with everyone. So, I think the jargon. You should be my someplace. So instead of also using acronyms, just simplify that and use the full name. But however, just use plain simple English that everybody can understand because I know I get very confused when I speak to an IT person and I'm like oh you just lost me there. I don't know what you're saying. Are you speaking another language? So just to simplify the language? I think we'll make a difference".

Some interviewees suggested glossaries of terms and using synonyms except where one did not exist to simplify jargon or technical terms.

One interviewee differed with the prevailing opinion on this question and responded by stating that currently, IT is pervasive across the industry and workplaces and abbreviations and technical terms are increasingly commonplace and maintained that they are understood by all since the technology they pertain to, is inherently used widely.

Another interviewee suggested the organisation hold workshops from time to time and discuss new acronyms and technical terms and the concepts they represent. While this will likely not be implemented, it does indicate that abbreviations and jargon to distract from policy intent and should be avoided.

The overall view expressed was that jargon and technical terms should be avoided at all costs, except where not possible and in these cases, glossaries were required including examples, since simply expanding an acronym did not mean readers knew what they meant.

4.11.5 If IT security awareness specifically could be improved, what would that entail in your opinion?

Some interviewees answered this question by stating that their view was that policy awareness was adequate and they had no other suggestions to provide about how it could be improved.

Nonetheless, some valuable views were provided by the remaining interviewees who suggested moving away from online training to discuss security principle and concepts. The view was that Information security is already a specialised domain within IT and any attempt to canvass awareness through online training was counterproductive. It only served to confound and confuse staff who were already extremely cautious and averse to the use of technology in the workplace in lieu of manual processes.

Many stated that the current method of employing training awareness was flawed since no background was provided and staff were automatically enrolled for information security training without understating why. Many stated that unless they had leaked information or had access to data they should not have, they should not be targeted with training.

The underlying consensus was that the quizzes provided at the end of training interventions online served no purpose since staff simply attempted the training to "tick the box" and answered the questions/quizzes till they passed the quiz, because it was mandatory.

This underlines an important aspect identified through the interviews where staff felt they were often subjected to information security training with no context on how it would impact them or why they were required to do so. Making training mandatory satisfies the compliance and attestation principles but may not necessarily communicate intent and expected outcomes to staff. Additionally, staff preferred a combination of online and face to face training where questions could be posed and there would be more interaction between security experts/staff and staff. One interviewee stated, "boring and bland presentations simply won't cut it anymore".

One interviewee suggested “behind-the-scenes” training where staff could ask questions to security experts within the organisation responsible of the implementation of actual information security technology.

While interviewees shared views on increasing frequency of training and awareness initiatives, many did not want to be subjected to more online training although one interviewee suggested “Popups on PCs about security related things”.

Many viewed the current nature of information security training to be impaired with too much emphasis on online training solely and a general lack of face-to-face training.

One interviewee summed up the overall views on training awareness as “there’s already a lot, training on self service. All employees don’t actually absorb it. How old you are, how tech savvy you are, what department you are in all affect the absorption.”

4.11.6 In your opinion, are there adequate opportunities available to you to shape our IT Security programme or for your input to be incorporated?

There were mixed opinions provided about whether employees had avenues available to them to provide feedback or input on information security as a discipline.

Many stated that if there were opportunities available to them, they were not familiar with these which underlines another important outcome from the research in that while it is possible to create feedback mechanisms for staff, if the awareness of said mechanisms remains low or non-existent then no feedback can and will be received. The implication is that in designing feedback strategies for staff, staff should be included or consulted around what will be considered practical and thus yield beneficial feedback which can serve to improve the impact made not only by awareness initiatives but underscore the policy intent and objectives as a whole. Many stated that if staff existed to whom feedback on information security could be provided, they did not know these staff. This therefore indicated that once again, even if there was feedback or input from staff, they did not know who to provide it to. Therefore, feedback mechanisms should be agnostic of the “people” element although one interviewee suggested ensuring the organisation had information security champions who were designated in every business unit to whom

feedback could be provided. This can be summed by one response verbatim, “no, I don’t know who to contact to make any suggestion to, there is no platform to suggest something”. This view was common with staff initially hesitating to answer or waiting to be prompted while they thought about the response and was characterised by the following response:

“With the assessments, I think that's where we normally do it, but honestly, I don't think there is a way per se to say I can log this. Maybe I'm just not aware of it. Where you can log in initiative in terms of IT think maybe that part.” This quote encapsulates the view that employees did not often think they had a contribution to make in terms of advancing information security programmes across the organisation. Many views centred around the fact that staff in general trusted that “someone” was carefully analysing the programme and its intent and reworking or amending accordingly the input from “other” staff and ensuring efficacy.

There was a common view that “experts” deal with specialised matters such as Information Security as a discipline and this work was best left to them and ordinary “unspecialised” staff would not have much to contribute to the discourse on this subject.

Some interviewees stated that they did not consider themselves information security experts and therefore could not provide feedback.

This also highlights the fact that some staff do not understand the role they play in information security and therefore only view themselves as unimportant components of the ISMS versus vital actors with vital roles to play, including but not limited to providing valuable user feedback insofar as the ISMS and its implementation is concerned.

A handful of interviewees further qualified their responses by stating that there was inadequate time for information security training, since it was seen as an overhead and further stated that with busy schedules and daily duties there was insufficient time to provide feedback.

11 out of 45 interviewees stated that they did feel there were adequate opportunities available to them to provide input and feedback.

4.11.7 Where would you locate our Information Security policy?

In order for staff to read the information security policy, they must know where to locate/source it. Only 16 out of 45 staff knew where the policy was located, representing only 35.5% of interviewees. This also indicates that while in general, staff understood information security as a discipline as well as the purpose of information security policy as it pertained to keeping an organisation safe from threats, including having opinions on how to improve awareness and provide feedback, more than half of the interviewed staff did not know where to locate the policy itself.

While knowing where a document is located is not an indicator of a successful ISMS implementation, it is imperative that policies and documents intended for all staff are easily accessible and, in a location, familiar to them.

It is also possible that the staff who did not know where to locate the policy have only seen the policy document once, at onboarding where it is mandatory to sign-off and attest having read the document. This also indicates that any subsequent revisions made to the document since joining are not familiar to the employee.

The majority of employees who indicated that they could not locate the policy tended to think an “internal only” policy was published on the public facing website.

Policies are to be read by all, but more importantly understood by all, and it appears that while the policy could not be located by all interviewed, or even read by all interviewed, the underlying policy intent was well entrenched and implemented, nonetheless.

4.12. Interview Analysis and coding

Within the context of qualitative research analysis, where large textual data sets must be analysed to identify key themes, outcomes and potential study variables, coding is used. Coding qualitative data is an essential step in the research process, as it enables the systematic organization, analysis, and interpretation of large sets of text-based data which

is uniquely difficult and complex (Given, 2020) to analyse and cannot be subjected to quantitative analysis methods.

Coding involves the assigning of labels or codes to different segments of qualitative data, thereby facilitating data organization and analysis. It involves breaking down the data into smaller units, identifying patterns, and as a result can be useful in generating meaningful themes or categories. Coding allows researchers to explore relationships including potential causative effects and to discover insights, and derive conclusions that may not be immediately obvious from simply reading the data alone (Braun and Clarke, 2019).

Nvivo is a widely used software tool designed specifically for qualitative data analysis. Numerous studies have highlighted the benefits of using Nvivo for qualitative data analysis (Saldaña, 2021). Researchers have reported increased efficiency, improved organization, and enhanced analytical rigor when employing Nvivo in their studies.

All the transcripts from the interviews were imported into Nvivo and a word cloud was generated seen in Figure 4.12.

Figure 4.12: Word cloud

The generation of word clouds when analysing qualitative data is useful in that it graphically groups commonly grouped or appearing words (representing themes and ideas) together with the most frequent words appearing different (larger in this case) versus less commonly appearing words. In order to generate this word cloud, the questions were omitted from the coding since they would skew the results in that were posed to all respondents and would therefore appear as a result in each transcript. Using the word cloud enables the contextualisation of significant or meaningful ideas from the interviews (Baseley, 2013).

One of the main themes identified from the word cloud was that " *Information security policy and systems need improvement and simplified for employees to understand.".*

With this framing, a set of codes was developed and analysed. This included creating a frequency of items which aligned with each of the identified codes. This is presented below in Figure 4.13.

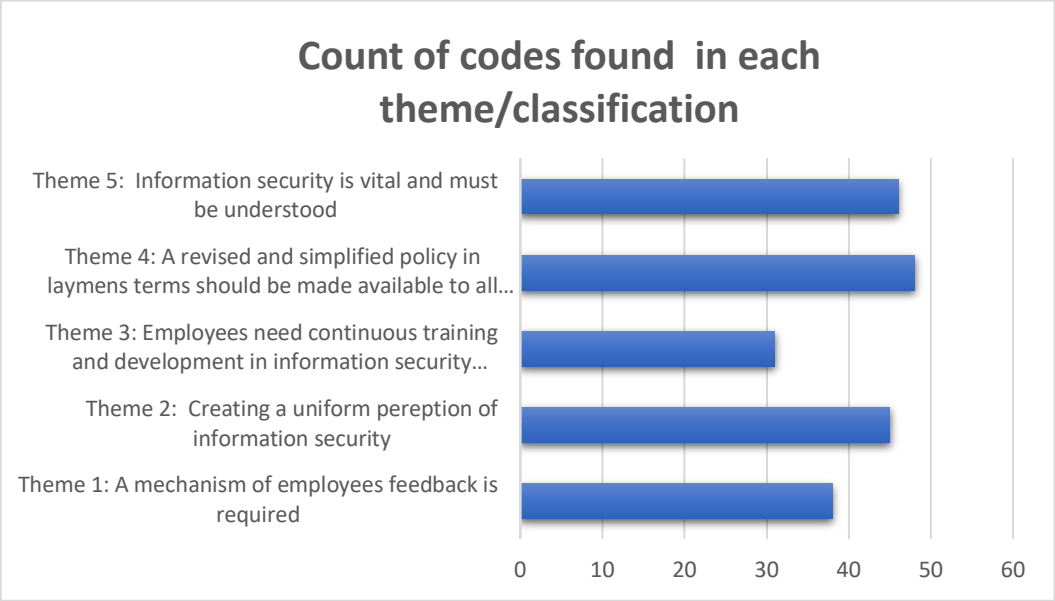

Figure 4.13: Frequency of items in each code.

This figure provides an indication of overall themes as a consequence of the classification of data into the individual codes established and from the framing statement.

These over-arching themes are identified as follows and emanate from the total interview output:

Theme 1: A mechanism for employee feedback is required
Theme 2: Creating a uniform perception of information security
Theme 3: Employees need continuous training and development in information security awareness.
Theme 4: A revised and simplified policy in laymens terms made available to all employees
Theme 5: IT Security is vital and must be understood.

4.12.1 Theme 1: A mechanism for employee feedback is required

The coding of interviews indicated that a number of respondents felt that inadequate mechanisms were available to provide feedback on information security and its related disciplines. Moreover, these staff felt that even if there were mechanisms for them to provide feedback, they were either unaware of them or did not feel that it was adequately communicated and easily available. This has significant correlation to the fact that many viewed information security as a detailed and specialised body of knowledge, with some respondents indicating that they considered themselves average employees and therefore they would unlikely have significant or material contributions to make to improve the information security programme. Moreover employees confirmed that even though they did not know of feedback or improvement mechanisms, they assumed that the programme was inherently adequate saying, “I am sure a good job is being done” while at the same time stating, “I don’t think there’s chances for staff to participate in feedback”

Given the number of responses and overall sentiment regarding feedback, it is vital that any conceptual framework developed for improving the construct pertaining to design, rollout and measurement of policy success include a suitable feedback or improvement mechanism. Organisations ordinarily perform satisfaction surveys regarding culture and ethics on an ongoing basis in order to satisfy regulatory scrutiny around responsibility to manage these expected outcomes. Therefore the organisation has the “machinery” to create similar surveys for information security policy feedback and gather opinions from staff on what is considered to be working and not working. These surveys will need to

carry the relevant scientific rigour and adjust or normalise data across expected normality but will result in not only valuable insight to the internal functioning of the programme as viewed by employees, but will also show employees that their opinions are valued and taken into account.

4.12.2 Theme 2: Creating a uniform perception of information security

Evident from the interviews was that perceptions around information security were varied. There were a number of views where employees felt there was not enough being done to protect sensitive information and data. This included interactions both internally and externally. Further to this, some employees held the opinion that too much was being done where it pertained to technologies such as encryption, password security, multi-factor authentication and general computer use. The view here was characteristic of bureaucracy and tardiness, in the time these technologies impeded staff from performing daily duties. Further staff explained that they viewed the organisation at the forefront of information security practices especially where online security was concerned but once again, strong views pervaded the interviews around the "cost" associated with these technologies and how they impacted and interfered with daily duties. Interestingly, staff viewed internal repositories for policies and documents as inadequate stating they were hard to navigate to and often contained out-dated information. This then highlights the result that perceptions across the interviews were not homogenous and the conceptual framework must include components that work to counteract this. This can include the rationalisation of technologies using the security "Onion" of layers where potentially numerous system logins per day (as expressed by staff) can be resolved. In addition, these perceptions were both positive and negative and this links directly to the first theme, that allows for staff to communication potentially impaired perceptions and views to security professionals and policy designers who can create mechanisms to resolve same.

4.12.3 Theme 3: Employees need continuous training and development in information security awareness

Closely aligned to perceptions was the theme centred around training and awareness. Employees believed largely that training and awareness initiatives were inadequate given the changing nature of technology. This was specifically mentioned with the context of cyber related security. Employees felt unsafe and unsure around their responsibilities on

a daily basis insofar as information security was concerned. Questions specific to this were around employees understanding implications in daily tasks and duties. Here interviewees responded generally stating they broadly understand the use of passwords, security mechanisms and system based logging and auditing. Further than this, there was the perception that ongoing training specifically classroom based, or face to face training was severely lacking. Interviewees viewed online training as unable to convey important new information to staff adequately. The other question relating directly to this theme was that of training frequency. Employees did not or could not remember attending formal training in the last 12 months. Most cited online training which they viewed as mandatory but not value-additive. Views concentrated on the fact that these online training modules that the organisation employed did not facilitate qualitative mechanisms for information sharing. There were no opportunities for clarification and cyber related issues were not explained in anecdotes and examples. This left significant gaps in staff views around the adequacy of training and the frequency, format and content thereof. Consequently from a theoretical framework point of view the theme of continuous education training and awareness is significant given the direct "touch-points" with staff. Essentially, the training and awareness is the only other formal discourse mechanisms between policy creators and policy consumers. If it is flawed or inadequate as well then employees view the security programme as unlikely to be effective. It is for this reason that the conceptual framework must include components around training, awareness and where possible face-to-face training for all staff.

4.12.4 Theme 4: A revised and simplified policy in laymens terms made available to all employees

The overwhelming contingent of interviewees viewed the policy as convoluted, difficult to read and complex. This points directly to impaired readability and comprehension in that even though the CDA methods define the document as difficult to read, many staff admitted to having read, but not understood it. The central view was that the document contained too many technical terms and acronyms. Furthermore, apart from the codified language used in the document, staff said they were unable to interpret the desired outcomes from staff. While they all knew they had to comply and compliance was not optional, many struggled with understanding exactly how compliance would be achieved. Many respondents stated categorically that the document needed to be rewritten to remove acronyms, jargon and abbreviations and use simple language with particular

examples to explain difficult or specialised expected behaviour. Laymen's terms was often used to define the way the policy was to be rewritten. Some interviewees mention that current policies are already simplified and understandable, while others suggest that aligning the language with what employees are familiar with can be beneficial.This theme had the highest number of code count and is characteristic of a fundamental problem affecting the readability and thus comprehension of the policy. It is therefore crucial that the conceptual framework include a suitable component to deal with policy refinement and ongoing maintenance. The ongoing maintenance is important in that as the demographic or characteristic of the staff population change and adapt to differing conditions, so too must the policy and its design variables. This means that even though policies are subjected to ongoing review as is the case with many corporate documents, it will be essential to reconsider the target audience each time. IT will not be possible to create policies that stratify the population since this then negatively impacts the common perception and views that are central to maintaining a unified organisational approach to information security.

4.12.5 Theme 5: IT Security is vital and must be understood

This theme was also characterised by a high coding number indicative of a general common view that information security as it pertains to the organisational context. Here respondents believed that the value of information security was without debate especially given the nature of the organisation's business and its clients. Moreover, given the regulatory and market scrutiny all employees who participated in the interviews agreed that the importance of information security could not be underestimated although some said they didn't necessarily understand the frameworks and broader body of knowledge, only indicating limited understanding in a finite context as it pertained to them. While it is unimportant that all employees familiarise themselves with frameworks and methods, it is important that they understand the organisational security programme is based on sound fundamentals and best practice. Moreover, a direct implication of security conversations creates in the mid of respondents, a link to protection of personal information and data confidentiality. In this context or framing, most employees who made the link viewed information security as critical to ensure suitable controls were in place and could be reported on. This was to prevent sensitive data from being leaked and used for fraud and reputational losses. Many respondents responded indicated that while

they valued the technologies keeping data safe, they often lacked an understanding of how they functioned, what rules were defined and how information may be treated securely both internally and externally. One interviewee described IT security as the responsibility of IT professionals to protect information online and offline. This accurately encompasses much of the sentiment in response to the questions around utility, effectiveness and importance. The conceptual model as a consequence includes IT security as a central component with other constructs and characteristic working to not only advance its imperative but to advance it as a discipline within the organisation as well.

These emanating and identified themes, in terms of the research objective must then be incorporated to formulate the conceptual/theoretical model answering the research questions.

4.13 Comparative analysis of data

Given the analysis of all collected and analysed data within the study, it is crucial to compare the results from each research instrument to create a cohesive outcome (Donahue and Cropf, 2014). In addition data triangulation methods define "following a thread" as a viable mechanism to analyse and triangulate the various data sets from the mixed methods approach.

The result from the Fry Index, the SMOG Index as well as the Cloze deletion test all characterise the information security policy as "difficult to read" requiring post graduate level education as the minimum reading level. In addition, the results of the Cloze deletion test confirmed that respondents were materially unable to accurately guess the missing word in most cases with no responses 100% accurate across the sample. Overall, the conclusion from the CDA tests indicate a general impairment in the language, tone, grammar and text used within the policy which is at odds with its "applies to all staff, contractors and 3rd parties" stipulation. The remaining survey questions posed to staff indicate an overall trend or themes centring around a general familiarity with the policy including an affirmation of understanding and impaired accessibility to said policy.

So basically, it can be seen that most staff within the sample, if the CDA methods are relied on, cannot read the policy for meaning or guess missing words, but are familiar with the policy and its implications on daily duties even though it is not easily accessible and responses indicate mixed views as to readability and comprehension. Most however believe there is inadequate awareness about the policy and confirm that better ways to communicate the document must be sought. Exactly half of all respondents believe the language and grammar is adequate and concise but most do not believe policy authors and experts have done enough to avoid confusing terms and jargon. Finally, the majority of respondents to the survey confirmed they attended information security training in the preceding 12 months.

This contrasts the views in the qualitative interviews significantly with interview coding then enabling the development of themes which counteract many of the assertions from the likert-scale section of the survey. This is not uncommon since each of the methods contains within various underlying strategies to collect data about the study variables and while the modes to collect data differ, the underlying constructs are scientifically sound and can differ (Krosnick and Presser, 2010).

4.14 Outcomes for main research objectives

Various approaches have been used to provide analysis and context around the Information Security Policy being analysed. This has included A Fry Readability Score, a scoring according to the SMOG Index as well as a Cloze deletion test and survey as well as interviews. Therefore, and in order to suitably answer the core research questions, the outcomes from the various research instruments are used to answer the research questions and offer potential solutions in order to achieve the overall research objective.

4.13.1 Objective One

The initial objective was to use the various research instruments to confirm or refute whether the use of jargon and specific language detracts from or conversely supports the communication of intent of a said IT security policy/procedure. Outcomes from the Fry's readability and SMOG test both independently of each other, corroborate the outcome that the current policy is difficult to read with a high level of reading proficiency required and at minimum requiring a university post graduate qualification. This means that the

policy includes difficult and technical language and therefore any reader without the requisite minimum education level will experience potential difficulty in reading the policy for understanding and is therefore unlikely to understand how the said policy intent impacts his/her daily duties.

Moreover, the inference is that since all staff cannot understand the policy, it is likely that those staff may not necessarily adhere to the policy thereby exposing the organisation to risk beyond its appetite from an information security perspective. This also means that awareness of the implications of the policy stipulations may invariably be overlooked in day-to-day tasks and duties resulting in potential information security policy breaches ultimately impeding the effectiveness of the ISMS and ISO 27001 compliance. For a large financial institution, this directly creates challenges in ensuring overall adherence to the underlying frameworks that ISO 27001 as a domain rely on as well.

Consequently, it is foreseeable that the policy must be revised to remove jargon, complex technical terms, jargon and more simply communicate the policy intent.

Interviewees responded heavily with indications that jargon should be removed at all lengths and where it was impossible to do so, like is the case with technical terms, glossaries and example are to be provided.

4.13.2 Objective two

The second objective involved identifying the appropriate mechanisms to ensure that the intent of an information technology policy is conveyed and what methods are to be used. If policy comprehension itself is problematic and not effective, then what other methods can be used, and will that result in improved information security policy implementation by itself? Based on the surveys and interviews, a significantly evident outcome was that the Information Security policy was not only difficult to read, but not easily accessible with respondents indicating that the policy authors have not done enough to avoid acronyms, abbreviations, and technical language even though most survey respondents indicated having attended Information Security training in the last 12 months.

Awareness is a significant contributor to overall ISMS implementation success with high levels of awareness directly correlated to successful policy implementation and improved

end user security outcomes. Employees who attend more frequent training across various Information Security topics retain the knowledge better and are more likely to make the right choices where information security impact their daily tasks and duties.

Where interviewees were asked how information security awareness could be improved, strong views were held around increasing frequency, enhancing simplicity, and avoiding the exclusive use of online training methods. There was a definite consensus that online training provided no adequate feedback mechanism for staff and removed the ability for staff to clarify understanding of complex principles and concepts.

For information security intent to be clearly and effectively communicated, policy and related documents must be easily readable by all staff, training must be contextual, and employees must be engaged to educate them around the background and motivations of specific training interventions and more specifically how they align to policy and overall security management intent. Any ISMS implementation which has the Deming cycle included but does not provide well-advertised and communicated mechanisms for feedback misses a significant step required in the continuous improvement loop from the user/consumers perspective.

4.13.3 Objective three

The final objective of the research was the development of a conceptual or theoretical framework that will aid the organisation in developing information security policies and procedures that are easily understood by all staff in order to ensure a robust ISMS programme and a well communicated overall information security management intent. This objective is discussed in the section below.

4.15 Proposed conceptual framework outcomes

The development of a theoretical framework relies on interpreting the data informing potential solutions to the problem, into a theory about how the problem may be solved (Varpio et al., 2019) which is called the subjectivist inductive approach. Theoretical frameworks are developed a priori or through theoretical deduction or even may be developed before data collection whereas a conceptual framework provides a relationship

analysis between the various variables involved in the study and in relation to the research problem (Grant and Osanloo, 2014). Therefore, for this study and in order to satisfy the original aims and objectives, a conceptual framework has been developed.

Within the context of the study a number of important and noteworthy outcomes have been established. The first outcome is that the Information security policy is not readable at every staff member in the organisation as interrogated by Fry's readability instrument and corroborated by the SMOG and Cloze test where respondents could not accurately guess-replace deleted words. Surveys indicated that respondents did not believe policy authors and writers had done enough to avoid confusing acronyms and abbreviations and views around clarity and conciseness of messages was not overwhelmingly positive. Therefore, any conceptual framework must provide a dimension in order to remediate the readability challenges.

The other established outcome pertains to awareness and socialisation/training pertaining to policies, where respondents did not believe awareness of information security policies was adequate and accessibility was viewed as problematic. Confirmed by the interviews where most staff did not know where to locate the policy/ies. Moreover, staff believed the frequency with which training was conducted was inadequate including views expressed around online training being impersonal and not providing adequate opportunities for staff to ask questions and seek clarity. Therefore, the conceptual framework must include a dimension which caters to socialisation of policy and its intent adequately.

The third established outcome was that information security policy is viewed as a specialised and niche discipline even though it applied to all staff as users of data across the organisation. Respondents did not feel included in the development of policy, understood its background and underlying concepts adequately and did not feel that any suggestions they had to improve the information security programme or ISMS could be directed anywhere. If users are the weakest link (Bulgurcu, Cavusoglu and Benbasat, 2010), then any conceptual framework which does not incorporate users is inherently flawed.

Finally, the identified themes from the qualitative data inform the overall conceptualisation of a framework since they indicate vital ideas/problems and constructs that the model must solve for.

These themes included:

Theme 1: A mechanism for employee feedback is required

Theme 2: Creating a uniform perception of information security

Theme 3: Employees need continuous training and development in information security awareness.

Theme 4: A revised and simplified policy in laymens terms made available to all employees

Theme 5: IT Security is vital and must be understood.

This data then enables the formation of a multi-dimensional conceptual framework for improving information security policy creation, readability, comprehension and ongoing maintenance thereof.

4.14.1 Multi-dimensional conceptual framework for information security management

Given the 3 outcomes from the research and the 5 key themes emanating from the interviews, it was possible to formulate a multi-dimensional framework including the various desired outcomes and themes – which tackle problems that must be solved by the conceptual framework.

The attribution of components/outcomes to each dimension is as follows:

Dimension 1: Employee Engagement and Communication

- Component 1: Employee feedback
  Component 2: Creating a uniform perception of information security
- Component 7: Readability

This dimension focuses on fostering employee engagement and effective communication within the organization. It involves creating channels for employees to provide feedback,

ensuring a unified perception of goals and values, and promoting clear and understandable communication materials.

Dimension 2: Knowledge and Awareness

- Component 3: Continuous awareness and education
- Component 6: Users

This dimension emphasizes the importance of continuous learning, awareness, and education. It involves implementing programs and initiatives that promote ongoing education and development for employees. Additionally, it highlights the need to consider the users' perspective and tailor knowledge-sharing approaches to their needs. This dimension also provides fit for purpose and simple feedback mechanisms for staff to ask clarifying questions or make suggestions. It is also, potentially anonymous.

Dimension 3: Policy and Process Optimization

- Component 4: Simplification of policy

This dimension focuses on simplifying policies and processes to enhance efficiency and effectiveness within the organization. It involves reviewing and streamlining policies to reduce complexity, eliminate unnecessary bureaucracy, and facilitate better decision-making. Further to this, policy creation/drafting removes jargon, ambiguity and acronyms for a unified and concise result benefitting directly the readability and thereby the comprehension of the documents it produces.

Dimension 4: Security and Risk Management

- Component 5: IT Security at the center of everything

This dimension underscores the significance of IT security and risk management across all aspects of the organization. It involves integrating robust security measures into every aspect of operations, including technology systems, processes, and employee behaviours.

By integrating these components into the multi-dimensional framework, it is possible to address key areas of employee engagement, communication, knowledge management, policy optimization, and security within the organization.

Consequently, a multi-dimensional theoretical framework for policy creation and readability has been developed and is depicted below:

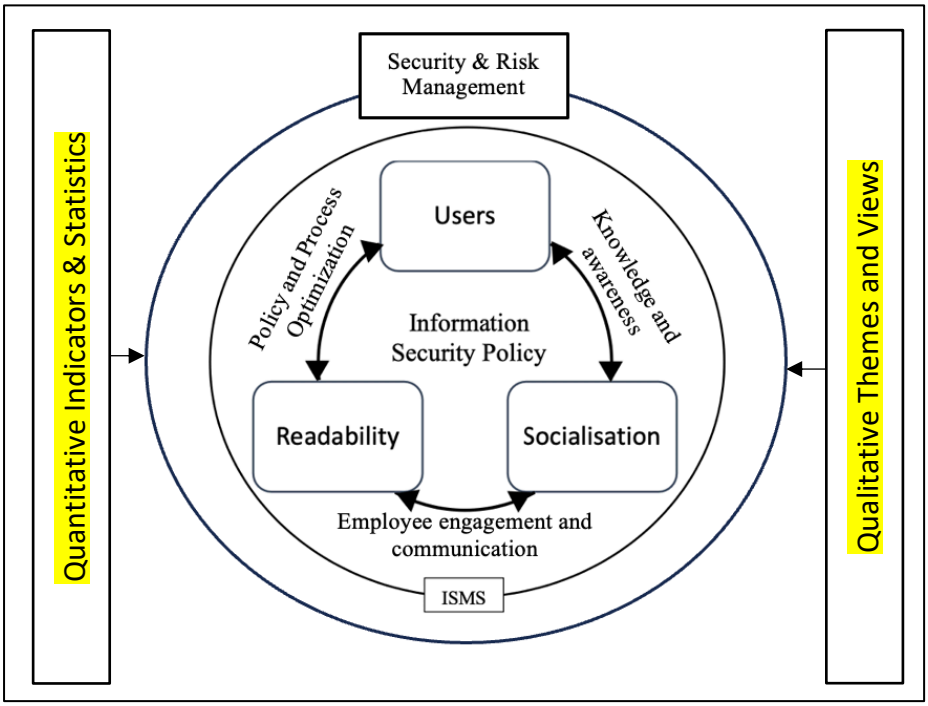

Figure 4.14: Multi-Dimensional Conceptual Framework for Information Security Policy Management

As can be seen within the framework there are links between the 4 dimensions and each other since all 4 dimensions are critical to the proper functioning of the framework. While policy creators could create policies, without subjecting them to readability instruments, would result in the challenges currently existing. Important feedback loops are depicted by the links between the dimensions to ensure that users have the ability to influence readability before the policy is subjected to an instrument as well as after. Socialisation will involve ensuring that general training and awareness involves users before training is rolled out to all staff in a focus group setting to elicit response and feedback and allow for adjustments and improvements. Focus groups are also suggested via the framework to ensure that once policy is defined and both before and after readability instrument analysis occurs, focus groups opine on whether the actual and original security management intent is maintained and if the document itself is concise and accurate.

Users and Socialisation are impacted by the Knowledge and Awareness Dimension due to the direct relation users have with assisting policy creators refine content, define concise policies and are also impacted by the outcomes of socialisation, since once

communicated they form part of organisational discourse on information security and the socialisation aspect becomes self-propagating.

Readability is closely correlated to Socialisation through employee engagement and communication which involves employee feedback loops and enabling the formation of uniform perceptions across the organisation.

Equally important and related is the relationship between Readability and Users where the Dimension of Policy and Process Optimisation allows users to directly influence Readability through direct or indirect access to policy creators who enable optimization and refinement on an ongoing basis.

All the Dimensions are thus contained within the encompassing Dimension of Security and Risk Management which is the underlying domain of practice and expertise. Within this encompassing domain lies all discourse (written or verbal), standards, policies, mechanisms, programmes and stakeholders.

The conceptual framework also includes 2 pillars, namely the Quantitative pillar and the Qualitative pillar. These empirical phases of the study were critical in facilitating reliable but also rich views insofar as the research questions and aims are concerned. These must therefore be incorporated where applicable into the framework when used to inform a representative and in-depth view. Since the creation of policies is cyclical in nature involving a creation, refinement and potentially a retirement phase, incorporating these two pillars are essential in the organisational construct given the changing and evolving nature of the document over time as well as changing and evolving views internally. Notwithstanding the internal flux, external contributing factors are likely to change over time necessitating an ongoing approach that takes into consideration qualitative and quantitative sources of input.

In the quantitative pillar, insights have formed a foundational layer for the subsequent qualitative phase by identifying potential influential factors and informing the selection of critical dimensions to be explored in-depth. The quantitative results thus served as a quantitative backdrop, enriching the qualitative investigation by highlighting focal points for more nuanced exploration of the problem and its various facets. The qualitative phase of the study entailed in-depth interviews and content analysis of relevant texts. This phase aimed to provide a comprehensive understanding of the underlying contexts, meanings, and social dynamics that shape the subject matter.

By delving into participants' perspectives and analysing textual artifacts, this phase unearthed intricate insights that go beyond statistical associations. The qualitative findings have enriched the quantitative patterns with interpretative depth, thereby allowing for the emergence of a multi-dimensional framework that encapsulates both numerical trends and nuanced contextual understandings. The synthesis of quantitative and qualitative findings has enabled the triangulation of insights, resulting in a holistic and refined framework that accurately represents the complexities of the studied phenomenon.

In summary, the conceptual framework developed aims to ensure the 4 dimensions established as such, via the research study are synergised while still operating within the confines of the ISMS and therefore achieving an organisations' strategy to manage security appetite adequately and align to industry expectations and fulfil its obligations to customers and staff alike.

CHAPTER 5

Findings and recommendations

5.1 Introduction

Chapter five provides a summary and reconsiders the research questions in light of the results. This chapter critically assesses whether or not readability and comprehension of Information Security policies at the research organisation is indeed affected by the reading level of the reader, whether or not education levels impact this imperative and overall, what mechanisms must be implemented at the organisation in order to better ensure proper and inclusive implementation approaches are delivered. This chapter concludes by indicating possible future research proposals to mitigate existing literature gaps identified or evident in this research study.

5.2 Dissertation Conclusions

This case study aims to assess the comprehensibility of information security policies in a South African bank which has involved used scientifically approved tools and mechanisms to firstly analyse the policies including the use of Fry's Readability metric and the SMOG value. Thereafter the researcher compared the results of surveys where the Cloze deletion test was used. Finally, to balance the outcomes from the various scientific methods and surveys, interviews were conducted to further understand prevailing opinions and attitudes to information security policies within the organisation. Given the various sources of information an overall research outcome has been achieved.

Chapter One of the study has introduced the underlying thesis questions including, but not limited to areas where existing research has not been conducted to unpack the readability of information security policies in the context of organizational use. Further to this, the problem statement has been explored to develop the rationale behind the study.

Chapter Two has explored the existing literature with respect to the readability and comprehensibility studies including, but not limited to, the scientific models and methods as well as the various CDA instruments such as that of Fry, SMOG and Cloze tests. Additionally, the applicability of the rubrics has been considered in the development of an overall underlying context with which the study could be conducted. Finally, the ISO

standard has been analysed to determine whether specific mention is made in the standard around the applicability of comprehension and understanding, insofar as it relates to implementation of an ISMS and the success thereof.

Chapter Three defines the technical aspects of the study including research methodology design instrumentation sample population calculations sample size as well as ethical and data collection limitations.

Chapter Four details the collection of actual response data including the results from the SMOG index and that of the Cloze deletion test (surveys) as well as analysing the results from the interviews conducted. The results from the analysis of these sources of information as well as that of interviews informs the relevant outcomes for the main research objectives and possible solutions to the research hypothesis.

5.3 Limitations and potential future research

Research into the readability and comprehension of organisational policies is an exercise that is usually conducted internally to organisations and the results or outcomes of such studies are rarely, if ever made public, not only due to the confidential nature of the documents themselves but publishing externally around policy document impairments is less than ideal from an organisational standpoint. Therefore, it is difficult to state with finality whether other such studies have been conducted in organisations locally since no published material was available specific to the banking sector and more especially within the specialised context of information security and ISMS implementations.

In terms of limitations identified through the Cloze deletion test, it is important to point out that prior knowledge of the underlying domain body of knowledge can significantly influence a respondent's ability to understand a specific document or text. According to schema theory, readers rely on their existing knowledge and experiences to construct meaning from a text (Rumelhart, 1980). Therefore, when administering the Cloze readability test, it is essential to consider the respondents' prior knowledge and how it may affect their comprehension of the material. Given the survey results indicating knowledge and ignorance of the contents of the policy, it is vital to understand that respondents potentially guessed the deleted words correctly due to familiarity with the concepts. It is also entirely possible that the correctly guessed words were accurate purely

coincidentally, and therefore not associated to prior knowledge. Therefore a limitation is that simply because a word weas guessed correctly, or incorrectly, it is not adequate to state with certainty as to the underlying reason for the success guess or lack thereof.

It would also appear that respondents tend to familiarise themselves better with acronyms and jargon the longer they are within the employ of the organisation and may be further advanced by their proximity to information security discipline through their assigned duties or through engagement with information security resources and specialists which may occur on an ad-hoc basis. Consequently, without considering and accounting for these limitations it is not ideal to formulate any research outcomes or responses to the research aims and objectives.

The interviews were conducted remotely because of working from home practices and mobility arrangements where it was found that interviewees tended to be brief with their answers. It is possible that interviews conducted face to face may have yielded more information from interviewees. This is another limitation and potential future research involving the analysis of perceptions to information security informed by the mixed methods used in this study including the administering of Cloze deletion tests must consider the feasibility of conducting these interviews face-to-face.

5.4 Recommendations

The original hypothesis was that information security policies which are inherently specialised lack adequate readability and result in impaired comprehension as a consequence. Even though information technology has its own standards, frameworks and industry bodies there has been a lack of the creation of conceptual measurement criteria and specific imperatives for information security, to ensure the policies were adequately understood across varying levels of education and reading ability. This means that even though the documents are intended to be written for all staff, and the research has proven they are not, there are no mechanisms to resolve this problem permanently and repeatably. This directly impacts the ability of the policy and its intent to be communicated effectively and understood in the organisation. Moreover, this translates to the successful implementation of the ISMS and the policy and results is better outcomes overall for the organisation in achieving its objectives of managing information security well since awareness is an influential component but not the only component.

The research provides insight around staff perceptions to information security policies as well as an indication of the readability of the in-scope policy and provides suggestions on the amendment of the policy to simplify the language, reduce the use of acronyms as well as providing management and information security specialists in the organisation with further suggestions from the interviews on how to better manage awareness, communication, and training around information security policy. This will allow a more robust ISMS implementation and create a workforce more capacitated to understand how their daily duties are impacted by, and impact information security tangibly.

5.4.1 Recommendations for policy creators

Given the responses from respondents, results from Fry's readability index and the SMOG Index as well as the results from the Cloze deletion test policy creators can rewrite policies to:

- Simplify complex language to ensure policies are written to be read and understood by all staff regardless of educational level and qualifications;
- Remove or avoid unnecessary acronyms which do not enhance the readability of the policies;
- Shorten the Information Security policy to improve its familiarity within the organisation and move purely technical content to baseline standards for implementation;
- Create focus groups of staff to assist with simplifying content and proofing revisions to ensure readability is ensured without losing the context or intent. These groups must be of a diverse and inclusive nature in composition and should preferably exclude staff who have been within the employ of the organisation for any length to remove familiarity bias.
- Policy creators can also use industry bodies and other forums where information security is topical such as SABRIC IT working groups to ensure lessons learned at other banks and financial services institutions are incorporated as practices to formulate and promulgate information security policies.

5.4.2 Recommendations for ISMS managers and specialists

Awareness was identified through the interviews as a significant contributor to respondents' familiarity with policy content, but more especially with how the content impacted their daily duties. Essentially, many interviewees indicated that they did not view information security policy as relevant to their daily duties since they did not work in IT. While a misconception since anyone who has access to information in an organisation falls within the scope of applicability, this does represent an important problem to resolve. It is recommended that training initiatives are created to unpack the security policy intent and use scenarios to communicate the applicability to staff. This will take the form of distilling the policy into key statements/objectives and simplifying this into principles for staff. These principles must be simple, avoid acronyms and use examples to educate staff on what they mean and how staff have an important role to play in ensuring they are achieved.

Moreover, simply simplifying the policy into statements will not be adequate and the next step will be to identify measurement criteria to evaluate the success of their entrenchment in the organisations. This will require the use of key data sources which rely on easily replicable calculations to inform success or failure. This will involve identifying what specially should be measured, how to measure it, and tolerance levels to indicate whether improvement is required, or success has been achieved. This will involve continuous improvement and refinement to fully deliver improving results and to create indicators for ISMS managers and implementors as well as policy creators to indicate whether the policy, statements, and underlying implementation is aligned since it is possible that the policy is clear, readable and well-constructed, but not communicated well and may result in a failed ISMS programme, worse, it may result in a deterioration of the control environment since staff can subvert technological controls and weaken the organisations defences.

Ensuring adequate opportunities are available for employees to pose questions and seek clarity is pivotal. Many interviewees did not believe there were adequate processes in place to ensure this. Many did not feel they had anyone to direct their queries around information security which highlights that ensuring an adequate feedback and suggestion loop is required. This can take the form of a shared email account used internally only where staff can submit queries to. Additionally, it is recommended that individual

champions/representatives for information security are identified, provided training, and introduced to staff to facilitate an adequate feedback and improvement mechanism available to staff.

Finally, a noteworthy outcome from the interviews was that respondents did not know where to locate/source the Information Security policy. It is recommended that policies are located in a location internally that is found easily or navigated to, more simply. While some interviewees knew the policy was on the Intranet, they did not know where. Many believed the policy was available to download on the organisations public facing website which is not the case. Some organisations have resolved this by creating a shortcut on every user's desktop which cannot be deleted enabling simpler navigation and alleviating any confusion around where the policies are located. This also solves for employees who do not have their own computers and instead potentially share a computer.

5.4.3 Recommendations for line managers and staff

Relying only on policy creators and security specialists for the implementation of the recommendations misses an important role that staff, and their line managers play in ensuring a successful ISMS programme within the organisation. By including more roleplays, organisations stand a chance at staying ahead of enemies (Potter, 2008). Therefore, staff must read information security policies on an going basis or whenever there is an update/revision. Typically training interventions are rolled out around phishing, hacking, sharing confidential information and other topical issues in the organisation. These training interventions are mandatory, and all staff are required to comply. There is no annual attestation performed by all staff for the Information Security Policy and while it is likely that staff have read the policy, there is no guarantee that all staff have read it and no mechanisms to ensure they read it on a frequent (at minimum annual) basis. In addition, line managers can perform the oversight function to ensure the Information Security policy has been read. Provided the abovementioned recommendations around policy creation are implemented, the organisation is able to ensure that policy is readable/comprehensible across all levels, can easily be located, is read annually (or another reasonable frequency) and can then measure compliance using predetermined measurement criteria, since mobilization results in better management, more so when measured (Catasús et al., 2007). These key indicators serve to inform an overall implementation key success factor.

5.5 Conclusion

With banks and financial services institutions entrusted with the confidential and private information of its customers, it is not only critical for these organisations to protect said information, but legally mandated as well. To this end, the successful implementation of a programme to manage said information relies primarily on the overall strategy in the organisation expressed in policies, standards, statements, training material and presentations and other artefacts. Ensuring that the policies are readable across all levels of the organisation remains a critical success factor in firstly ensuring the policies are understood. It is only after being understood, that they can be implemented. The lack of analysis of Information Security policies from a readability/comprehension point of view indicates that this is not something considered by policy creators, implementers, specialists, and other stakeholders charged with ensuring information is treated adequately internally and ensuring all staff behave accordingly. Where employees do not know where to locate policies and potentially have not read same, a deficiency in ISMS implementation exists. While efforts are made to simplify the imperatives into training interventions, adequately doing so may detract from the original policy intent, this then creates a disconnect between policy and implementation. Employees then do not understand the relationship between information security and their daily duties and may act to counteract the policy intent unintentionally or through ignorance. This ultimately can result in data breaches, financial loss and pervasive reputational loss as well. This may have negative impacts on the organisations ability to remain competitive and ultimately achieve its growth strategy.

REFERENCES

2022 Cost of Data Breach Study: Impact of Business Continuity Management. (2022). [online] Available at: https://www.ibm.com/downloads/cas/AEJYBPWA.

AbuSaad, B., Saeed, F., Alghathbar, K. and Khan, B. (2011). Implementation of ISO 27001 in Saudi Arabia – obstacles, motivations, outcomes, and lessons learned. Australian Information Security Management Conference. [online] doi:10.4225/75/57b52709cd8b2.

Alderson, J.C. (1979). The Cloze Procedure and Proficiency in English as a Foreign Language. TESOL Quarterly, 13(2), p.219. doi:10.2307/3586211.

Alkhurayyif, Y., Weir, G. R. S. (2018). Evaluating readability as a factor in information security policies. International Journal of Trend in Research and Development, 54-64.

Alkhurayyif, Y., Weir, G., Toolan, F. (2017). Using sequential exploratory mixed methods design to explore readability of ISPs. In 2017 IEEE Trustcom/BigDataSE/ICESS (pp. 1163-1168). IEEE.

Almeida, F. (2018). Strategies to perform a mixed methods study. DOI:10.5281/zenodo.1406214

Almutairi, A., & Alshammari, M. (2019). Readability and Comprehensibility of the ISO/IEC 27001:2013 Information Security Management System Standard. Journal of Information Privacy and Security, 15(3), 123-135.

Alotaibi, M., Furnell, S. and Clarke, N. (2016). Information security policies: A review of challenges and influencing factors. 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST). doi:10.1109/icitst.2016.7856729.

Alshammari, A., Rasli, A., Alnajem, M., Arshad, A. (2014). An Exploratory Study on the Relationship between Organizational Innovation and Performance of Non-profit Organizations in Saudi Arabia. Procedia - Social and Behavioral Sciences. 129. 10.1016/j.sbspro.2014.03.674.

Alshammari, M., & Almutairi, A. (2020). The Effect of Visual Aids on the Comprehension of the ISO/IEC 27001:2013 Information Security Management System Standard. Journal of Information Privacy and Security, 16(1), 1-13.

Alshammari, M., & Almutairi, A. (2021). The Effect of Plain Language on the Comprehension of the ISO/IEC 27001:2013 Information Security Management System Standard. Journal of Information Privacy and Security, 17(1), 1-12.

An Assessment of Drivers, Constraints and Opportunities Overcoming Poverty and Inequality in South Africa. (2018). [online] Available at: https://documents1.worldbank.org/curated/en/530481521735906534/pdf/124521-REV-OUO-South-Africa-Poverty-and-Inequality-Assessment-Report-2018-FINAL-WEB.pdf.

Anderson, R. (2001). Why Information Security Is Hard – An Economic Perspective. Proceedings of the 17th Annual Security Applications Conference (ACSAC) (pp358-365).IEEE.

Andress, A. (2003). Surviving Security. Auerbach Publications. doi:10.1201/9780203501405.

Agresti, A. (2002). Categorical Data Analysis (2nd ed.). Wiley.

Ardalan, A., Ardalan, R., Coppage, S. and Crouch, W. (2007). A comparison of student feedback obtained through paper-based and web-based surveys of faculty teaching. *British Journal of Educational Technology*, *38*(6), pp.1085-1101.

Babbie, E. (2016). The Practice of Social Research (14th Ed.). Cengage Learning.

Badarudeen, S. and Sabharwal, S. (2010). Assessing Readability of Patient Education Materials: Current Role in Orthopaedics. Clinical Orthopaedics and Related Research®, [online] 468(10), pp.2572–2580. doi:10.1007/s11999-010-1380-y.

Baldwin, J.R., Pingault, JB., Schoeler, T. Protecting against researcher bias in secondary data analysis: challenges and potential solutions. Eur J Epidemiol **37**, 1–10 (2022). https://doi.org/10.1007/s10654-021-00839-0

Baseley, P. (2013). Qualitative data anali=ysis with Nvivo. Sage.

Beavers, AS, Lounsbury, JW, Richards, JK, Huck, SW, Skolits, GJ and Esquivel, SL, 2013. Practical considerations for using exploratory factor analysis in educational research. Practical Assessment, Research, and Evaluation , 18 (1), p.6.

Bhandari, P. (2023, January 16). Triangulation in Research. Guide, Types, Examples. Scribbr. https://www.scribbr.com/methodology/triangulation/

Björnsdottir, S.H., Jensson, P., Thorsteinsson, S.E., Dokas, I.M. and de Boer, R.J. (2022). Benchmarking ISO Risk Management Systems to Assess Efficacy and Help Identify Hidden Organizational Risk. *Sustainability*, *14*(9), p.4937.

Bland, J. M., Altman, D. G. (1995). Comparing methods of measurement: why plotting difference against standard method is misleading. The Lancet, 346(8982), 1085-1087.

Boehmer, W. (2008). Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001. 2008 Second International Conference on Emerging Security Information, Systems and Technologies. doi:10.1109/securware.2008.7.
Bote, D., (2019). The South African National Cyber Security Policy Framework: a Critical Analysis (Doctoral dissertation, North-West University (South Africa).).
Bratus, S., Burkhart, M., Shubina, A., Williams, L. (2016). Cybersecurity meets psychology: Cognitive security metrics. Journal of CyberSecurity. DOI: 10.1093/cybsec/tyv008
Braun, V., Clarke, V. (2019). Reflecting on reflexive thematic analysis. Qualitative Research in Sport, Exercise and Health, 11(4), 589-597.
Broderick, J.S. (2006). ISMS, security standards and security regulations. Information Security Technical Report, 11(1), pp.26–31. doi:10.1016/j.istr.2005.12.001.
Brown, T.A. (2015). Confirmatory Factor Analysis for Applied Research. Guildford Publications.
Bryman, A. and Cramer, D. (2009). Quantitative data analysis with SPSS 14, 15 and 16 : a guide for social scientists. London ; New York: Routledge.
Bujang, M. A., Omar, E. D., Baharum, N. A. (2018). A review on sample size determination for Cronbach's alpha test: a simple guide for researchers. The Malaysian Journal of Medical Sciences: MJMS 25(6), 85.
Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 34(3), p.523. doi:10.2307/25750690.
Cain, K. (2006). Children's reading comprehension difficulties: A comprehensive meta-analysis. The Science of Reading: A Handbook (pp. 431-456). Blackwell Publishing.
Cairney, P. (2015). The politics of evidence-based policy making. Palgrave Macmillan.
Calder, A. and Watkins, S. (2012). IT Governance. Kogan Page Publishers.
Carr, J. (2012). Inside cyber warfare. Beijing ; Sebastopol, Ca: O'reilly.
Catasús, B., Ersson, S., Gröjer, J. and Yang Wallentin, F. (2007). What gets measured gets … on indicating, mobilizing and acting. Accounting, Auditing & Accountability Journal, 20(4), pp.505–521. doi:10.1108/09513570710762566.
Cavusoglu, H., Mishra, B., Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 9(1), 69-104. DOI: 10.1080/10864415.2004.11044208
Cheng, W., Warren, M. (1999). Linguistic features of the TOEFL intermediate Cloze Test: Developing a profile of candidate proficiency. Language testing. 16(1), 1-31.
Christie, P. (2006). Changing regimes: Governmentality and education policy in post-apartheid South Africa. International Journal of Educational Development, 26(4), pp.373–381. doi:10.1016/j.ijedudev.2005.09.006.
Cochran, W.G. (2005). Sampling techniques. [online] New York: Wiley. Available at: https://www.wiley.com/en-us/Sampling+Techniques%2C+3rd+Edition-p-9780471162407.
Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? Information Security Technical Report, [online] 14(4), pp.186–196. doi:10.1016/j.istr.2010.04.004.
Coolican, H. (2017). Research Methods and Statistics in Psychology. [online] Psychology Press. doi:10.4324/9780203769836.
Courtis, J.K. (1995). Readability of annual reports: Western versus Asian evidence. Accounting, Auditing & Accountability Journal, 8(2), pp.4–17. doi:10.1108/09513579510086795.
Creswell, J.W. and Creswell, J.D. (2018). Research design: Qualitative, quantitative, and Mixed Methods Approaches. 5th ed. Thousand Oaks, California: SAGE Publications.
Cronbach, L.J. (1951). Coefficient alpha and the internal structure of tests. Psychometrika, 16(3), pp.297–334. doi:10.1007/bf02310555.
Cudeck, R., 2000. Exploratory factor analysis. In Handbook of applied multivariate statistics and mathematical modeling (pp. 265-296). Academic Press.
Culot, G., Nassimbeni, G., Podrecca, M. and Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. The TQM Journal, 33(7), pp.76–105. doi:10.1108/tqm-09-2020-0202.
Davis, T.C., Wolf, M.S., Bass, P.F., Middlebrooks, M., Kennen, E., Baker, D.W., Bennett, C.L., Durazo-Arvizu, R., Bocchini, A., Savory, S. and Parker, R.M. (2006). Low literacy impairs comprehension of prescription drug warning labels. Journal of General Internal Medicine, 21(8), pp.847–851. doi:10.1111/j.1525-1497.2006.00529.x.

Derguech, W., Zainab, S.S. e and D'Aquin, M. (2018). Assessing the Readability of Policy Documents. Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, pp.247–256. doi:10.1145/3209415.3209498.

Desmedt, O., Heeren, A., Corneille, O. and Luminet, O., 2022. What do measures of self-report interoception measure? Insights from a systematic review, latent factor analysis, and network approach. *Biological Psychology*, p.108289.

DeVellis, R. F. (2016). Scale development: Theory and applications (4th ed.). SAGE Publications.

Doak, C.C., Doak, L.G., Friedell, G.H. and Meade, C.D. (1998). Improving comprehension for cancer patients with low literacy skills: strategies for clinicians. CA: A Cancer Journal for Clinicians, 48(3), pp.151–162. doi:10.3322/canjclin.48.3.151.

Doherty, N., Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. Computers & Security. 25. 55-63. 10.1016/j.cose.2005.09.009

Dombora, S. (2016). Characteristics of Information Security Implementation Methods.

Donahue, P.J., Cropf, R.A. (2014). Integrating quantitative and qualitative data: an introduction to mixed methods in public administration and public policy. Public Administration Review, 74(3) pp.399-407.DOI10.1111/puar.12219

Dorner, D.G. and Gorman, G.E. (2006). Information Literacy Education in Asian Developing Countries: cultural factors affecting curriculum development and programme delivery. IFLA Journal, 32(4), pp.281–293. doi:10.1177/0340035206074063.

Duke, N.K., Ward, A.E., & Pearson, P.D. (2021). The Science of Reading Comprehension Instruction. Read Teach, 74(6), 663– 672. https://doi.org/10.1002/trtr.1993

Elleman, A. M., & Oslund, E. L. (2019). Reading Comprehension Research: Implications for Practice and Policy. Policy Insights from the Behavioral and Brain Sciences, 6(1), 3–11. https://doi.org/10.1177/2372732218816339

Entin, E.B. (1986). Using the cloze procedure with computer programs: a deeper look. ACM SIGCSE Bulletin, 18(1), pp.153–162. doi:10.1145/953055.5700.

Eybers, S., Mvundla, Z. (2022). Investigating cyber security awareness (CSA) amongst managers in small and medium enterprises (SMEs). In *Comprehensible Science: ICCS 2021* (pp. 180-191). Springer International Publishing.

Fairclough, N. (2001). Language and Power. Routledge.

Fairclough, N. (2007). Language and Globalization. Routledge.

Farn, K.-J., Lin, S.-K. and Fung, A.R.-W. (2004). A study on information security management system evaluation—assets, threat and vulnerability. Computer Standards & Interfaces, 26(6), pp.501–513. doi:10.1016/j.csi.2004.03.012.

Field, A. (2013). Discovering Statistics Using IBM SPSS Statistics. SAGE Publications Ltd.

Fielding, J. (2020). The people problem: how cyber security's weakest link can become a formidable asset. Computer Fraud & Security, 2020(1), pp.6–9. doi:10.1016/s1361-3723(20)30006-3.

Flowerday, S.V. and Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. Computers & Security, 61, pp.169–183. doi:10.1016/j.cose.2016.06.002.

Fry, E.B. (1989). Reading Formulas: Maligned but Valid. Journal of Reading, [online] 32(4), pp.292–297. Available at: http://www.jstor.org/stable/40029925 [Accessed 3 Nov. 2022].

Furnell, S. and Bishop, M., 2020. Addressing cyber security skills: the spectrum, not the silo. Computer fraud & security, 2020(2), pp.6-11.

Galdas, P. (2017). Revisiting Bias in Qualitative Research: Reflections on Its Relationship With Funding and Impact. International Journal of Qualitative Methods, 16(1).

Given, L. M. (2020). The SAGE Encyclopedia of Qualitative Research Methods. SAGE Publications.

Graesser, A.C., Singer, M., Trabasso, T. (1994). Constructing inferences during narrative text comprehension. Psychological Review. 101(3), 371-395.

Gravetter, F. J., & Wallnau, L. B. (2016). Essentials of Statistics for the Behavioral Sciences. Cengage Learning.

Grant, C. and Osanloo, A. (2014). Understanding, selecting, and integrating a theoretical framework in dissertation research: creating the blueprint for your 'house'. Administrative Issues Journal Education Practice and Research, [online] 4(2). Available at: https://files.eric.ed.gov/fulltext/EJ1058505.pdf.

Grobler, M., Jansen van Vuuren, J.C., Leenen, L. (2012). Implementation of a Cyber Security Policy in South Africa: Reflection on Progress and the Way Forward. 386. 215-225. 10.1007/978-3-642-33332-3_20.

Grossmann, M., 2021. How social science got better: Overcoming bias with more evidence, diversity, and self-reflection. Oxford University Press.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). Multivariate data analysis (8th ed.). Cengage Learning.
Hameed, Z., Counsell, S., Swift, S. (2013). An investigation into information security management in UK organizations: Practices, challenges, and financial losses. Information Management & Computer Security, 21(5), 334-356. DOI: 10.1108/IMCS-04-2013-0020
Hartz-Karp, J. and Marinova, D. (2017). Methods for Sustainability Research. Edward Elgar Publishing, pp.1–13.
Hayeri Khyavi, M. and Rahimi, M. (2015). The Missing Circle of ISMS (LL-ISMS). Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, pp.73–77. doi:10.1145/2751957.2751972.
Hoehe, M.R. and Thibaut, F. (2020). Going digital: how technology use may influence human brains and behavior. Dialogues in Clinical Neuroscience, 22(2), pp.93–97. doi:10.31887/dcns.2020.22.2/mhoehe.
Holmes, N. (2001). The great term robbery [computer jargon]. Computer, 34(5), pp.94–96. doi:10.1109/2.920619.
Honig, M.I. (2006). New Directions in Education Policy Implementation. State University of New York Press.
Howie, S., Combrinck, C., Roux, K., Mokoena, M. and Palane, M. (2016). PIRLS Literacy 2016: South African Highlights Report. [online] Available at: https://www.shineliteracy.org.za/wp-content/uploads/2018/01/pirls-literacy-2016-hl-report.zp136320.pdf.
Hudson, Bob & Hunter, David & Peckham, Stephen. (2019). Policy failure and the policy-implementation gap: can policy support programs help?. Policy Design and Practice. 2. 1-14. doi:10.1080/25741292.2018.1540378.
ISO (International Organization for Standardization (2018). Publicly Available Standards. [online] Iso.org. Available at: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip.
ISO. (n.d.). ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection. [online] Available at: https://www.iso.org/committee/45306.html.
Jamshed, S. (2014). Qualitative research method-interviewing and observation. Journal of Basic and Clinical Pharmacy, 5(4), pp.87–88. doi:10.4103/0976-0105.141942.
Janks, H. (1997). Critical Discourse Analysis as a Research Tool. Discourse: Studies in the Cultural Politics of Education, [online] 18(3), pp.329–342. doi:10.1080/0159630970180302.
Janks, H. (2009). Literacy and Power. Routledge.
Johnson, M. E., Goetz, E., Grosse, E. (2007). The strategic alignment of IT and business strategy in high-performing companies. Journal of Strategic Information Systems, 16(3), 337-364. DOI: 10.1016/j.jsis.2007.06.003
JTC 1. (n.d.). JTC 1 History – SD 2. [online] Available at: https://jtc1info.org/sd-2-history/.
Kaufmann, J. and Schering, A. (2007). Analysis of Variance ANOVA. Wiley Encyclopedia of Clinical Trials. doi:10.1002/9780471462422.eoct017.
Khando, K., Gao, S., Islam, S.M. and Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: a systematic literature review. Computers & Security, 106. doi:10.1016/j.cose.2021.102267.
Kim, J.O., Ahtola, O., Spector, P.E., Kim, J.O., Mueller, C.W., 1978. Introduction to factor analysis: What it is and how to do it (No. 13). Sage.
Kline, R. B. (2015). Principles and practice of structural equation modeling (4th ed.). Guilford Press.
Knudsen, J.N., Löfgren, K. (2018). Critical discourse analysis for information security research: an introduction. Information Security Theory and Practicve. Lecture notes in Computer Science. Springer. DOI: 10.24251/HICSS.2017.058
Krosnick, J. A., Presser, S. (2010). Integrating Survey and Interview Data to Study Policy Deliberation. Research in Social Movements, Conflicts, and Change, 31, 109-143. doi:10.1108/S0163-786X(2010)0000031006.
Lenzini, G., Ryan, P.Y.A., Roll, A. (2014). Security in Computer Games: From Pong to Online Poker. CRC Press.
Leonard Grabeel, K., Russomanno, J., Oelschlegel, S., Tester, E. and Heidel, R.E. (2018). Computerized versus hand-scored health literacy tools: a comparison of Simple Measure of Gobbledygook (SMOG) and Flesch-Kincaid in printed patient education materials. Journal of the Medical Library Association, 106(1). doi:10.5195/jmla.2018.262.
Lumley, T., Diehr, P., Emerson, S., Chen, L. (2002). The importance of the normality assumption in large public health data sets. Annual Review of Public Health, 23, 151-169.

Lupton, D. (2010). Discourse analysis: a new methodology for understanding the ideologies of health and illness. Australian Journal of Public Health, 16(2), pp.145–150. doi:10.1111/j.1753-6405.1992.tb00043.x.
Machin, D., Mayr, A. (2012). How to do critical discourse analysis. Sage Publications.
Mahfuth, A., Yussof, S., Baker, A.A., Ali, N.A. (2017). A systematic literature review: Information security culture. In 2017 International Conference on Research and Innovation in Information Systems (ICRIIS) (pp. 1-6). IEEE.
Maroco, J., Garcia-Marques, T. (2013). Qualitative and Quantitative Research in Social Science: Common Features, Differences, and Goals. In J. Maroco (Ed.), Research Methods in Psychology (pp. 65-94). Springer.
Maxwell, S.E., Delaney. H.D. (2004) Designing Experiments and Analysing Data: A Model Comparison Perspective. Lawrence Erlbaum Associates.
Mc Laughlin, G.H. (1969). SMOG Grading-a New Readability Formula. Journal of Reading, [online] 12(8), pp.639–646. Available at: https://www.jstor.org/stable/40011226.
Moavenzadeh, J. (2015). The 4 th Industrial Revolution: Reshaping the Future of Production. [online] Available at: https://na.eventscloud.com/file_uploads/fe238270f05e2dbf187e2a60cbcdd68e_2_Keynote_John_Moavenzadeh_World_Economic_Forum.pdf.
Montero-Marin, J., Garcia-Campayo, J., Fajula, C., Gascón, S., Artal, J. (2019). Addressing researcher bias in social science research: Recommendations for researchers and reviewers. International Journal of Clinical and Health Psychology, 19(3), 244-252.
Monks, F.J. (1995). CREATIVITY: IDIOGRAPHIC VERSUS NOMOTHETIC APPROACH. European Journal of High Ability, 6(2), pp.137–142. doi:10.1080/0937445940060237.
Moodley, K., Pather, M. and Myer, L. (2005). Informed consent and participant perceptions of influenza vaccine trials in South Africa. Journal of Medical Ethics, 31(12), pp.727–732. doi:10.1136/jme.2004.009910.
Moore, D. S., McCabe, G. P., Craig, B. A. (2012). Introduction to the Practice of Statistics. W. H. Freeman and Company.
Moraka, L.I., Singh, U.G. (2023). The POPIA 7th Condition Framework for SMEs in Gauteng. In Computational Intelligence: Select Proceedings of InCITe 2022 (pp. 831-838). Singapore: Springer Nature Singapore.
Moran-Ellis, J., Alexander, V.D., Cronin, A., Dickinson, M., Fielding, J., Sleney, J. and Thomas, H., (2006). Triangulation and integration: processes, claims and implications. Qualitative research, 6(1), pp.45-59.
Naing, L., Winn, T.N. and Rusli, B. (2006). Practical Issues in Calculating the Sample Size for Prevalence Studies rusli nordin. Archives of Orofacial Sciences, pp.9–14.
Nietzio, A., Naber, D. and Bühler, C. (2014). Towards Techniques for Easy-to-Read Web Content. Procedia Computer Science, 27, pp.343–349. doi:10.1016/j.procs.2014.02.038.
Ojha, P.K., Ismail, A. and Kuppusamy, K.S. (2018). Perusal of readability with focus on web content understandability. Journal of King Saud University - Computer and Information Sciences. doi:10.1016/j.jksuci.2018.03.007.
Pallant, J. (2016). SPSS Survival manual: A step by step guide to data analysis using IBM SPSS (6th ed.). Open University Press.
Pashler, H., Bain, P. M., Bottge, B. A., Graesser, A., Koedinger, K., McDaniel, M., & Metcalfe, J. (2007). Organizing instruction and study to improve student learning: IES practice guide (NCER 2007-2004). Washington, DC: National Center for Education Research.
Paulsen, C. and Byers, R. (2019). Glossary of Key Information Security Terms. [online] csrc.nist.gov. Available at: https://csrc.nist.gov/publications/detail/nistir/7298/rev-3/final.
Perez-Guillermo, E., Rodriguez-Sanchez, C.M., Alfonseca, E., Rodrigues, P. (2015). Readability formulas for domain-specific texts: A Methodological proposal. Information Processing and Management. Doi:10.1016/j.ipm.2015.06.001
Perfetti C. A., Landi N., Oakhill J. V. (2005). The acquisition of reading comprehension skill. In Snowling M. J., Hulme C. (Eds.), The science of reading: A handbook (pp. 227-247). Oxford, UK: Blackwell.
Pimple, K.D. (2002). Six domains of research ethics. Science and Engineering Ethics, 8(2), pp.191–205. doi:10.1007/s11948-002-0018-1.
Plackett, R. L. (1983). Karl Pearson and the Chi-Squared Test. International Statistical Review / Revue Internationale de Statistique, 51(1), 59–72. https://doi.org/10.2307/1402731

Plate, A. (2011). ISMS: A Management Framework for Information Security. In: van Tilborg, H.C.A., Jajodia, S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-5906-5_289

Posey, C., Shoss, M. 2022. Research: Why Employees Violate Cybersecurity Policies. Harvard Business Review.

Potter, B. (2008). Is security really everyone's responsibility? Network Security, 2008(3), pp.9–10. doi:10.1016/s1353-4858(08)70030-8.

Pressley, M., Afflerbach, P. (1995). Verbal protocols of reading. The nature of constructively responsive reading. Lawrence Eribaum and Associates.

Redish, J.C. (1981). Understanding the limitations of readability formulas. IEEE Transactions on Professional Communication, PC-24(1), pp.46–48. doi:10.1109/tpc.1981.6447824.

Reynolds, K.A., Wry, E., Mullis, I.V.S., von Davier, M. (2022). PIRLS 2021 Encyclopedia: Education Policy and Curriculum in Reading. Retrieved from Boston College, TIMSS & PIRLS International Study Center website: https://pirls2021.org/encyclopedia.

Rosner, B. (2015). Fundamentals of biostatistics (8th ed.). Cengage Learning.

Rumelhart, D. E. (1980). Schemata: The building blocks of cognition. In R. J. Spiro, B. C. Bruce, & W. F. Brewer (Eds.), Theoretical issues in reading comprehension (pp. 33-58). Hillsdale, NJ: Lawrence Erlbaum Associates.

Ruxton, G.D. (2006). The unequal variance t-test is an underused alternative to Student's t-test and the Mann–Whitney U test. Behavioral Ecology, 17(4), pp.688–690. doi:10.1093/beheco/ark016.

Saldaña, J. (2021). The coding manual for qualitative researchers. *The coding manual for qualitative researchers*, pp.1-440.

Saunders, M., Lewis, P. and Thornhill, A. (2018). Research methods for business students. 4th ed. Harlow: Pearson Education.

Saunders, M.N.K. and Tosey, P. (2015). The Layers of Research Design. [online] Rapport. Available at: https://www.academia.edu/4107831/The_Layers_of_Research_Design.

Semenick, D. (1990). Tests and measurements: The T-test. Strength & Conditioning Journal, [online] 12(1), pp.36–37. Available at: https://journals.lww.com/nsca-scj/Citation/1990/02000/TESTS_AND_MEASUREMENTS__The_T_test.8.aspx.

Shanks, G. and Bekmamedova, N. (2018). Case study research in information systems. Research Methods, pp.193–208. doi:10.1016/b978-0-08-102220-7.00007-8.

Shin, S.-H. (2009). A Study on the Economic Benefits of Globalization: Focusing on the Poverty and Inequality between the Rich and the Poor. International Area Review, 12(2), pp.191–214. doi:10.1177/223386590901200210.

Shojaie, B., Federrath, H. and Saberi, I. (2015). The Effects of Cultural Dimensions on the Development of an ISMS Based on the ISO 27001. 2015 10th International Conference on Availability, Reliability and Security, [online] pp.159–167. doi:10.1109/ARES.2015.25.

Shorten, A. and Smith, J., 2017. Mixed methods research: expanding the evidence base. Evidence-based nursing, 20(3), pp.74-75.

Sibanda, L. (2014). The readability of two Grade 4 natural sciences textbooks for South African schools. South African Journal of Childhood Education, [online] 4(2), pp.154–175. Available at: http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S2223-76822014000200010&lng=en&tlng=en. [Accessed 3 Nov. 2022].

Siponen, M., Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487-502. DOI: 10.2307/25750794

Snyman, M.E. (Martha E. (2004). Using the printed medium to disseminate information about psychiatric disorders. repository.up.ac.za. [online] Available at: http://hdl.handle.net/2263/2929 [Accessed 3 Nov. 2022].

Stevens, J. P. (2012). Applied multivariate statistics for the social sciences (5th ed.). Routledge.

Surette Van Staden, S., Tshele, M., Dowse, C., Zimmerman, L. (2011). Summary report summary report south african children's reading literacy achievement. [online] Available at: https://www.ecexams.co.za/2012_Exam_Results/Reading%20Literacy%20Achievement%202011.pdf [Accessed 3 Nov. 2022].

Susanto, H. and Almunawar, Mohammad Nabil. (2020). Information Security Management Systems: A Novel Framework and Software as a Tool for Compliance with Information Security Standards. 10.1201/9781315232355.

Susanto, H., Almunawar, M. and Tuan, Y.C. (2011). Information Security Management System Standards : A Comparative Study of the Big Five. [online] www.semanticscholar.org. Available at: https://www.semanticscholar.org/paper/Information-Security-Management-System-Standards-

%3A-Susanto-Almunawar/1b583de114c74c7480e25eac6fee348af980d627 [Accessed 3 Nov. 2022].
Sweller, J., Ayres, P., Kalyuga, S. (2011). Cognitive Load Theory. Springer.
Taan, S. and Hajjar, E. (2018). _Published by European Centre for Research Training and Development UK (www.eajournals.org). International Journal of Quantitative and Qualitative Research Methods, [online] 6(1), pp.27–38. Available at: https://www.eajournals.org/wp-content/uploads/Statistical-Analysis-Internal-Consistency-Reliability-and-Construct-Validity.pdf.
Taber, K.S. (2017). The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. Research in Science Education, [online] 48(6), pp.1–24. doi:10.1007/s11165-016-9602-2.
Taherdoost, H. (2016). Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. [online] papers.ssrn.com. Available at: https://ssrn.com/abstract=3205035.
Tavakol, M. and Dennick, R. (2011). Making Sense of Cronbach's Alpha. International Journal of Medical Education, [online] 2(2), pp.53–55. doi:10.5116/ijme.4dfb.8dfd.
Taylor, W.L. (1953). 'Cloze Procedure': A New Tool for Measuring Readability. Journalism Quarterly, [online] 30(4), pp.415–433. doi:10.1177/107769905303000401.
Taylor-Clarke, K., Henry-Okafor, Q., Murphy, C., Keyes, M., Rothman, R., Churchwell, A., Mensah, G.A., Sawyer, D. and Sampson, U.K.A. (2012). Assessment of Commonly Available Education Materials in Heart Failure Clinics. Journal of Cardiovascular Nursing, 27(6), pp.485–494. doi:10.1097/jcn.0b013e318220720c.
Tourangeau, R., Conrad, F.G., Couper, M. (2013). The Science of Web Surveys. Oxford University Press.
Tu, Z., and Yuan, Y. (2014). Critical Success Factors Analysis on Effective Information Security Management : A Literature Review Completed Research Paper.
Van Dijk, T.A. (1993). Elite discourse and racism. Sage Publications.
van der Berg, S. and Gustafsson, M. (2019). Educational Outcomes in Post-apartheid South Africa: Signs of Progress Despite Great Inequality. South African Schooling: The Enigma of Inequality, pp.25–45. doi:10.1007/978-3-030-18811-5_2.
Varpio, L., Paradis, E., Uijtdehaage, S. and Young, M. (2019). The Distinctions between Theory, Theoretical Framework, and Conceptual Framework. Academic Medicine, 95(7), p.1.
Velasco, J., Ullauri, R., Pilicita, L., Jácome, B., Saa, P. and Moscoso-Zea, O. (2018). Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry. [online] IEEE Xplore. doi:10.1109/INCISCOS.2018.00049.
Waclawski, E. (2012). How I Use It: Survey Monkey. Occupational Medicine, 62(6), pp.477–477. doi:10.1093/occmed/kqs075.
Walker, R., Unterhalter, E. (2007). Amartya Sen's capability approach and social justice in education. Palgrave Macmillan.
Wambugu, J. (2006). Race, gender and intelligence: a comparative study of black, white and indian students' lay theories of intelligence. [online] Available at: https://researchspace.ukzn.ac.za/xmlui/bitstream/handle/10413/1896/Wambugu_Jacob_Ngunyi_2006.pdf?sequence=1&isAllowed=y [Accessed 3 Nov. 2022].
Wasti, S.P., Simkhada, P., van Teijlingen, E.R., Sathian, B., Banerjee, I. (2022). The Growing Importance of Mixed-Methods Research in Health. Nepal J Epidemiol. doi: 10.3126/nje.v12i1.43633. PMID: 35528457; PMCID: PMC9057171.
Watkins, M. W. (2018). Exploratory Factor Analysis: A Guide to Best Practice. Journal of Black Psychology, 44(3), 219–246. https://doi.org/10.1177/0095798418771807
Weak Security Controls and Practices Routinely Exploited for Initial Access. 2022. Cybersecurity & Infrastructure Security Agency - https://www.cisa.gov/uscert/ncas/alerts/aa22-137a
Wendler, M.C., (2001). Triangulation using a meta-matrix 1. Journal of advanced nursing, 35(4), pp.521-525.
Wessa, P. (2021). Cronbach Alpha - Free Statistics and Forecasting Software (Calculators) v.1.2.1. [online] www.wessa.net. Available at: http://www.wessa.net/rwasp_cronbach.wasp [Accessed 1BC].
Wilcox, R.R. (2009) Introduction to Robust Estimation and Hypothesis testing (3rd Edition). Academic Press.
Wilfred Molotja, T. (2020). An Exploration of the academic reading strategies of first year English Education students at a South African university. Journal of African Education, 1(2), pp.103–123. doi:10.31920/2633-2930/2020/1n2a5.

Wissing, G.-J., Blignaut, A.S. and Van den Berg, K. (2016). Using readability, comprehensibility and lexical coverage to evaluate the suitability of an introductory accountancy textbook to its readership. Stellenbosch papers in linguistics, 46(0). doi:10.5774/46-0-205.

Wodak, R. and Meyer, M. (2001). Methods of Critical Discourse Analysis. doi:10.4135/9780857028020.

Wood, A. (1998). Globalisation and the Rise in Labour Market Inequalities. The Economic Journal, 108(450), pp.1463–1482. doi:10.1111/1468-0297.00354.

Woolley, G. (2011). Reading Comprehension. In: Reading Comprehension. Springer, Dordrecht. https://doi.org/10.1007/978-94-007-1174-7_2

World Bank. (2022). New World Bank Report Assesses Sources of Inequality in Five Countries in Southern Africa. [online] Available at: https://www.worldbank.org/en/news/press-release/2022/03/09/new-world-bank-report-assesses-sources-of-inequality-in-five-countries-in-southern-africa#:~:text=South%20Africa%2C%20the%20largest%20country.

www.iso.org. (n.d.). ISO - ISO/IEC JTC 1 - Information technology. [online] Available at: https://www.iso.org/committee/45020.html?view=participation.

www.iso.org. ISO Survey of certifications to management system standards - Full results. [online]. Available at: https://www.iso.org/committee/54998.html?t=KomURwikWDLiuB1P1c7SjLMLEAgXOA7emZHKGWyn8f3KQUTU3m287NxnpA3DIuxm&view=documents#section-isodocuments-top

Yuanke, S., Wang, J., Dong, Y., Zheng, H., Yang, J., Zhao, Y., Dong, W. (2021). The Relationship Between Reading Strategy and Reading Comprehension: A Meta-Analysis. Frontiers in Psychology, volume 12. https://www.frontiersin.org/articles/10.3389/fpsyg.2021.635289. DOI=10.3389/fpsyg.2021.635289

Zaini, M.K., Masrek, M.N. (2013). Conceptualizing the relationships between information security management practices and organizational agility. 2013 International Conference on Advanced Computer Science Applications and Technologies (pp. 269-273). IEEE.

Zieky, M.J. (2001). Differential item functioning by item type and difficulty for open ended and multiple-choice questions. Applied Measurement in Education. 14(3),275-294.

APPENDIX

Appendix 1: Survey (Cloze deletion test)

Research Questionnaire - Information Security Policy Analysis

Policy Research Survey

As part of my continued professional development, I am currently completing a postgraduate degree at the University of Kwa-Zulu Natal. In order to obtain this qualification, I am required to conduct my own research study and have selected the Domain Information Technology Governance and policy.

This particular study will investigate and evaluate the comprehensibility (readability) of information security policies and procedures within FirstRand.

As a staff member at [redacted] you have been invited to participate in this study. Your participation in the study, which is completely voluntary, will help me to understand the extent and awareness around information security policy within the bank and mechanisms that can be used to improve and further enhance existing methods to design, communicate and test staff understanding where IT security policies are concerned.
Your participation will require you to answer some questions about yourself and your views and perceptions on Information Security policies.
There is also a "fill in the blank" section where you must guess the missing words from a policy extract.

Should you have any questions, please feel free to direct them to me via email.

OK

* 1. Please indicate your gender:

- ◯ Male
- ◯ Female
- ◯ Other
- ◯ Prefer not to say

* 2. Please select your age range

- ◯ 18 - 24 years old
- ◯ 25 - 34 years old
- ◯ 35 - 44 years old
- ◯ 45 - 54 years old
- ◯ 55 years old +

* 3. How long have you been employed at [redacted] its divisions or subsidiaries?

- ◯ 0 - 5 years
- ◯ 6 - 10 years
- ◯ 11 - 15 years
- ◯ 16 - 20 years
- ◯ 21 years +

* 4. Please indicate your education level:

- ◯ Primary school
- ◯ High school
- ◯ Undergraduate qualification
- ◯ Post graduate qualification

* 5. Are you familiar with the organisation's Information Security Policy and the updates made on an ongoing basis?

- ◯ Yes
- ◯ Somewhat
- ◯ Unsure
- ◯ Not really
- ◯ No

* 6. Do you understand the implications of the policies on the daily performance of your work/tasks?

- ◯ Yes
- ◯ Somewhat
- ◯ Unsure
- ◯ Not really
- ◯ No

* 7. Are the organisations information security policies easily accessible?

- ◯ Yes
- ◯ Somewhat
- ◯ Unsure
- ◯ Not really
- ◯ No

* 8. Are the information security policies easy to read and understand?

- ◯ Yes
- ◯ Somewhat
- ◯ Unsure
- ◯ Not really
- ◯ No

* 9. Do you believe there is adequate awareness around the information security policies within the organisation?

- ◯ Yes
- ◯ Somewhat
- ◯ Unsure
- ◯ Not really
- ◯ No

* 10. Are there are better ways for the organisation to communicate IT Security policies and the implications for you as an employee?

- ◯ Yes
- ◯ Somewhat
- ◯ Unsure
- ◯ Not really
- ◯ No

* 11. Is the overall language and grammar used within the IT security policies clear and concise?

- ◯ Yes
- ◯ Somewhat
- ◯ Unsure
- ◯ Not really
- ◯ No

* 12. Do you think the policy authors have done enough to avoid confusing acronyms and abbreviations used in Information Security Policies?

- ◯ Yes
- ◯ Somewhat
- ◯ Unsure
- ◯ Not really
- ◯ No

* 13. Have you attended any information security training, awareness or courses in the last 12 months?

- ◯ Yes
- ◯ Somewhat
- ◯ Unsure
- ◯ Not really
- ◯ No

* 14. ***The Following 3 Questions comprise the "Fill in the blank" section. Please fill in your best guess for the missing word indicated by (__XX__) into the corresponding numbered free text box below.***

Information must be protected (__1__) a manner commensurate with (__2__) sensitivity, value, and criticality. (__3__) measures must be employed (__4__) of the media on (__5__) information is stored (paper, (__6__) media, computer bits, etc.), (__7__) systems, which process it (__8__) , mainframes, voice mail systems, (__9__) .), or the methods by (__10__) it is moved (electronic (__11__) , face-to-face conversation, (__12__). Such protection includes restricting (__13__) to information based on (__14__) need-to-know principle. (__15__) policy is governed by (__16__) organisations (the group) Information (__17__) Governance Framework that supports (__18__) Risk Management and is (__19__) management tool to ensure (__20__) success. Information Security is (__21__) through the organisations Information (__22__) Management System, its related (__23__) , standards, control requirements and (__24__) . Each Business Entity must (__25__) familiar with the organisations (__26__) RACI Role Allocation, must (__27__) and update it according (__28__) organisational structures on a (__29__) basis.

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	

* 15. There are 3 (__30__) control objectives that address (__31__) Information Security requirements, which (__32__) as follows: Confidentiality - The (__33__) of data to those (__34__) to see it; Integrity - (__35__) the accuracy and (__36__) of information and processing (__37__); Availability - The property of (__38__) accessible and usable upon (__39__) by an authorised entity.

30	
31	
32	
33	
34	
35	
36	
37	
38	
39	

* 16. (__40__) policy applies to all (__41__) of organisation, as well (__42__) contractors and third-parties (__43__) their employees. This policy (__44__) also applicable to people, (__45__) and technology that manage (__46__) group's information systems and (__47__) resources including 4IR technology, (__48__) based and hosted infrastructure, (__49__), data and applications. End (__50__) must comply with this (__51__) as well as the (__52__) policies, standards and guidelines (__53__) interacting with group information (__54__) to maintain confidentiality, integrity (__55__) ensure appropriate availability.

40	
41	
42	
43	
44	
45	
46	
47	
48	
49	
50	
51	
52	
53	
54	
55	

DONE

Appendix 2: Policy extract used in Fry's readability calculation.

"Information must be protected in a manner commensurate with its sensitivity, value, and criticality. Security measures must be employed regardless of the media on which information is stored (paper, electronic media, computer bits, etc.), the systems, which process it (computers, mainframes, voice mail systems, etc.), or the methods by which it is moved (electronic mail, face-to-face conversation, etc.). Such protection includes restricting access to information based on the need-to-know principle. This policy is governed by the [redacted]

Information Technology Governance Framework that supports Enterprise Risk Management and is a management tool to ensure business success.

- *Information Security is managed through* [redacted] *Information Security Management System (ISMS), its related strategies, standards, control requirements and controls.*

- *Each Business Entity must be familiar with the* [redacted] *ISMS RACI Role Allocation, must review and update it according to organisational structures on a quarterly basis.*

Access to group information and resources must be restricted to those entities that have a legitimate business need and have been specifically authorized or granted through an approval process in accordance with the "Least Privilege" principle. Individual accountability (non-repudiation) must be assured at all times.

The Information Owners/System Owners must ensure that all system access privileges are removed as soon as they are made aware that the employee no longer needs the access.

The Information Owners/System Owners must ensure that system access privileges are suspended when employees proceed on their 10 consecutive days' annual leave. Business Entities may limit the system access that is restricted based on the individual business' requirements. The user is responsible for requesting re-instatement of this access on their return from leave.

Distribution of passwords must be done in a secure manner and to the intended user only.

Access must comply with legal, regulatory, statutory and contractual obligations. Access control mechanisms must adhere to the [redacted] *Functional Standard for Access and Authentication. The computer and communications system privileges of all users, systems, and independently operating programs (such as "agents") must be restricted based on the need-to-know. This means that privileges must not be extended unless a legitimate business-oriented need for such privileges exists.*

A formal process of re-certification/attestation to verify access rights given to end user within information processing resources must be completed at least bi-annually.

Users must ensure that storage and transportation of group information on removable media devices is done in a secure manner per the [redacted] Information Security Classification Functional Standard.

When removable media devices are used for backups, such backups must be with the consent of the Information Owner and the retention of data must comply with the group retention requirements.

When disposing of information storage media containing "Confidential" or "Restricted" group information as defined within the [redacted] Information Security Classification Functional Standard, it must be done as per the requirements in the [redacted] Policy on Secure Disposal of IT Assets and Information.

The group prohibits the use of mobile devices in high risk facilities containing information processing resources, storing, or transmitting classified information unless specifically permitted by the Risk Manager and Information Owner of that area. The group reserves the right to enforce restrictions on individuals permitted to use mobile devices in facilities containing information processing resources.

The group enforces the following restrictions on individuals permitted to use mobile devices in facilities containing information processing facilities, storing, or transmitting classified information.

- *Connection of managed devices to classified information systems must be approved by the system and information owner. The information stored on those devices are subject to random reviews/inspections by defined security officials, and if classified information is found, the incident handling policy is followed.*

Use of internal or external modems and wireless interfaces simultaneously within the mobile devices is prohibited while there is a connection to the group's internal network.

Refer to the [redacted] ISMS Functional Standard for Mobile Devices and Teleworking."

Appendix 3: Sample policy text word analytics

Total # of words: 566

Average # of words per sentence: 22
Total # of sentences: 26

Average # of syllables per word: 2
Total syllables in text: 1131

Total # of words with double syllables: 127
Percent of double syllables in text: 22%

Total # of words with single syllables: 292
Percent of single syllables in text: 52%

Total # of characters: 3296
Average # of characters per word: 5.8

Percent of 3+ syllables in text: 26%
Total # of words with 3+ syllables: 147

Full list of 3+ syllable words:

Information | protected | commensurate | sensitivity | criticality. | security | regardless | media | information | electronic | media | computer | computers | electronic | conversation | protection | restricting | information | principle. | policy | Information | Technology | Governance | Framework | Enterprise | Management | management | • information | Security | Information | Security | Management | related | strategies | requirements | Entity | familiar | Allocation | according | organisational | quarterly | information | restricted | entities | legitimate | specifically | authorized | approval | accordance | principle. | individual | accountability | repudiation | Information | Owners/System | Information | Owners/System | consecutive | annual | Entities | restricted | individual | business' | requirements. | responsible | requesting | instatement | distribution | regulatory | statutory | contractual | obligations. | mechanisms | Functional | Authentication. | computer | communications | independently | operating | restricted | legitimate | oriented | certification/attestation | verify | information | processing | completed | annually. | transportation | information | removable | media | Information | Security | Classification | Functional | removable | media | Information | retention | retention | requirements. | disposing | information | media | containing | "Confidential" | "Restricted" | information | Information | Security | Classification | Functional | requirements | Policy | Disposal | Information. | prohibits | facilities | containing | information | processing | transmitting | classified | information | specifically | permitted | Manager | Information | reserves | restrictions | individuals | permitted | facilities | containing | information | processing | following | restrictions | individuals | permitted | facilities | containing | information | processing | facilities | transmitting |

Total # of unique words: 237

All unique words: information | must | be | protected | in | a | manner | commensurate | with | its | sensitivity | value | and | criticality. | security | measures | employed | regardless

| of | the | media | on | which | is | stored | paper | electronic | computer | bits | etc. | systems | process | it | computers | mainframes | voice | mail | or | methods | by | moved | face | to | conversation | such | protection | includes | restricting | access | based | need | know | principle. | this | policy | governed | [redacted] | group | technology | governance | framework | that | supports | enterprise | risk | management | tool | ensure | business | success. | • information | managed | through | system | isms | related | strategies | standards | control | requirements | controls. | • each | entity | familiar | raci | role | allocation | review | update | according | organisational | structures | quarterly | basis. | resources | restricted | those | entities | have | legitimate | been | specifically | authorized | granted | an | approval | accordance | "least | privilege" | individual | accountability | non | repudiation | assured | at | all | times. | owners/system | owners | privileges | are | removed | as | soon | they | made | aware | employee | no | longer | needs | access. | suspended | when | employees | proceed | their | 10 | consecutive | days' | annual | leave. | may | limit | business' | requirements. | user | responsible | for | requesting | re | instatement | return | from | distribution | passwords | done | secure | intended | only. | comply | legal | regulatory | statutory | contractual | obligations. | mechanisms | adhere | functional | standard | authentication. | communications | users | independently | operating | programs | "agents" | know. | means | not | extended | unless | oriented | exists. | formal | certification/attestation | verify | rights | given | end | within | processing | completed | least | bi | annually. | storage | transportation | removable | devices | per | classification | standard. | used | backups | consent | owner | retention | data | disposing | containing | "confidential" | "restricted" | defined | disposal | assets | information. | prohibits | use | mobile | high | facilities | storing | transmitting | classified | permitted | manager | area. | reserves | right | enforce | restrictions | individuals | resources. | enforces | following | class.

Total # of repeat words and times repeated: 329

information(20) | must(18) | be(11) | in(8) | a(8) | manner(3) | with(5) | its(2) | and(15) | security(5) | of(12) | the(35) | media(5) | on(11) | which(3) | is(8) | electronic(2) | computer(2) | etc.(3) | systems(3) | process(3) | it(5) | mail(2) | or(5) | by(3) | face(2) | to(16) | such(4) | access(10) | based(3) | need(4) | principle.(2) | this(3) | policy(2) | [redacted](7) | group(10) | that(9) | risk(3) | management(3) | ensure(4) | business(5) | through(2) | system(5) | isms(3) | control(2) | requirements(2) | resources(3) | restricted(3) | entities(2) | have(2) | legitimate(2) | specifically(2) | individual(2) | at(2) | all(3) | owners/system(2) | owners(2) | privileges(5) | are(4) | as(5) | when(3) | their(2) | leave.(2) | requirements.(2) | user(3) | for(4) | re(2) | done(3) | secure(3) | comply(2) | functional(3) | standard(2) | users(2) | unless(2) | within(2) | processing(4) | storage(2) | removable(2) | devices(5) | per(2) | classification(2) | backups(2) | owner(2) | retention(2) | containing(4) | use(3) | mobile(3) | facilities(4) | storing(2) | transmitting(2) | permitted(3) | restrictions(2) | individuals(2) |

Appendix 4: 30 Sentences from Information Security Policy used in SMOG Test

Sentence number	Sentence
1	Information must be protected in a manner commensurate with its sensitivity, value, and criticality.
2	Security measures must be employed regardless of the media on which information is stored (paper, electronic media, computer bits, etc.), the systems, which process it (computers, mainframes, voice mail systems, etc.), or the methods by which it is moved (electronic mail, face-to-face conversation, etc.).
3	Such protection includes restricting access to information based on the need-to-know principle.
4	This policy is governed by the [redacted] Information Technology Governance Framework that supports Enterprise Risk Management and is a management tool to ensure business success.
5	Information Security is managed through the [redacted] Information Security Management System (ISMS), its related strategies, standards, control requirements and controls.
6	Each Business Entity must be familiar with the [redacted] ISMS RACI Role Allocation, must review and update it according to organisational structures on a quarterly basis.
7	This policy applies to all employees of [redacted] , as well as contractors and third parties and their employees.
8	This policy is also applicable to people, processes and technology that manage the group's information systems and data resources including 4IR technology, cloud based and hosted infrastructure, systems, data, and applications.
9	End Users must comply with this policy as well as the related policies, standards and guidelines when interacting with group information resources to maintain confidentiality, integrity and ensure appropriate availability.
10	All instances of non-compliance with this standard, whether intentional or not, must be identified by the Business Entity.
11	Information must be backed-up in a secure and reliable manner to ensure that business operation is not impaired in the event of information loss.
12	Backups must be performed in accordance with a defined back-up retention cycle that reflects business needs and considers the criticality of the information.
13	The frequency of backups must support a recovery time to limit business impact to an acceptable level.
14	Backup procedures must be documented. Backup procedures must be designed in such a way to ensure compliance with the [redacted] Data Backup and Recovery Technical Security Standard.
15	Regular restore testing must be done to ensure recovery and retrieval is possible in the event of data loss.
16	Tests must evaluate if data confidentiality and integrity is maintained during recovery or retrieval and that it may be done within an acceptable

	timescale (i.e., the point beyond which unacceptable loss would be suffered).
17	Onsite and offsite restore procedures must be in place to support the restore and recovery objectives of the overall business continuity or disaster recovery plan.
18	Group information stored locally on user computers and share drives must be backed-up on a regular basis to the group network.
19	The responsibility for this process lies with the End User.
20	Information security status information must be gathered to enable compliance measurement against group policy and standards, best practice, legal and statutory requirements.
21	Such risks must be assessed at an early stage of the process, documented, and reviewed at key stages during the development/implementation lifecycle.
22	Action must be taken to minimise risks by considering alternative approaches, revising staffing arrangements or plans and cancelling activities with unacceptable risks.
23	Prior to introduction of new information system development changes, a formal approved test procedure must be performed.
24	Where there is a requirement for testing to be done using “live” or production data, this must be requested, assessed and approved by the System Owner, Business CIO and ISO.
25	Deployment into the live production environment must be done in accordance with the Change Management Policy and Guidelines.
26	No part of this document may be reproduced, transferred, sold, or otherwise disposed of, without the written permission of the group.
27	This document can be used and copied within the group only.
28	However, no copies can be forwarded to any person who is not an employee or agent of the group without the prior written approval of the group.
29	This document, once downloaded from the document management system, is an uncontrolled copy, which is no longer guaranteed to be authoritative.
30	To ensure the use of the authorised copy, please download the document by accessing it via Information Security & Technology Policies and Standards on SharePoint.

Appendix 5: SMOG Complex Syllabic words

Information	protected	commensurate	sensitivity
Recovery	Technical	Security	regular
policy	contractors	policy	applicable
alternative	revising	arrangements	cancelling
disaster	Technology	Governance	Framework
availability	recovery	information	locally
document	compliance	intentional	identified
quarterly	otherwise	permission	document
considering	principle	restricting	conversation
compliance	overall	recovery	unacceptable
SharePoint.	integrity	accordance	guidelines
continuity	Policy	familiar	production
appropriate	according	documented	requirements
Guidelines	lifecycle	acceptable	statutory
organisational	documented.	protection	frequency
minimise	information	procedures	electronic
procedures	objectives	interacting	timescale
Policies	confidentiality	environment	policies
Security	Management	Entity	deployment
accessing	Allocation	requirements	strategies
computer	development/	electronic	policy
authorised	implementation	downloaded	media
guaranteed	procedures	regardless	information
criticality	management	possible	considers
recovery	security	introduction	accordance
processes	retrieval	management	operation
activities	unacceptable	responsibility	compliance
Enterprise	regular	reliable	information
computers	approval	document	Management
Entity	media	confidentiality	procedure
however	recovery	technology	infrastructure
acceptable	applications	development	including
related	requirement	authoritative	retrieval
requested	enable	criticality	integrity
measurement	retention	uncontrolled	evaluate

Appendix 6: Cloze Deletion Test

Information must be protected (__1__) a manner commensurate with (__2__) sensitivity, value, and criticality. (__3__) measures must be employed (__4__) of the media on (___5__) information is stored (paper, (__6__) media, computer bits, etc.), (__7__) systems, which process it (__8__) , mainframes, voice mail systems, (__9__) .), or the methods by (__10__) it is moved (electronic (__11__) , face-to-face conversation, (__12__). Such protection includes restricting (__13__) to information based on (__14__) need-to-know principle. (__15__) policy is governed by (__16__) organisations (the group) Information (__17__) Governance Framework that supports (__18__) Risk Management and is (__19__) management tool to ensure (__20__) success. Information Security is (__21__) through the organisations Information (__22__) Management System, its related (__23__) , standards, control requirements and (__24__) . Each Business Entity must (__25__) familiar with the organisations (__26__) RACI Role Allocation, must (__27__) and update it according (__28__) organisational structures on a (__29__) basis. There are 3 (__30__) control objectives that address (__31__) Information Security requirements, which (__32__) as follows: Confidentiality - The (__33__) of data to those (__34__) to see it; Integrity - (__35__) the accuracy and (__36__) of information and processing (__37__); Availability - The property of (__38__) accessible and usable upon (__39__) by an authorised entity. (__40__) policy applies to all (__41__) of organisation, as well (__42__) contractors and third-parties (__43__) their employees. This policy (__44__) also applicable to people, (__45__) and technology that manage (__46__) group's information systems and (__47__) resources including 4IR technology, (__48__) based and hosted infrastructure, (__49__), data and applications. End (__50__) must comply with this (__51__) as well as the (__52__) policies, standards and guidelines (__53__) interacting with group information (__54__) to maintain confidentiality, integrity (__55__) ensure appropriate availability.

Appendix 7: Deleted word Answers

Deleted word (Every 5th)	Word	Deleted word (Every 5th)	Word
1	in	29	quarterly
2	its	30	security
3	security	31	the
4	regardless	32	are
5	which	33	Restriction
6	electronic	34	authorised
7	the	35	safeguarding
8	computers	36	completeness
9	etc	37	methods
10	which	38	being
11	mail	39	demand
12	etc	40	This
13	access	41	employees
14	the	42	as
15	This	43	and
16	[redacted]	44	is
17	Technology	45	processes
18	Enterprise	46	the
19	a	47	data
20	business	48	cloud
21	managed	49	systems
22	Security	50	Users
23	strategies	51	policy
24	controls	52	related
25	be	53	when
26	ISMS	54	resources
27	review	55	and
28	to		

Appendix 8: Cloze deletion test responses

Word Deleted	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Response 1	in	data	security	extensively	where	digital	information	securely	radio	digital	format	electronic	access	user privileds	information	firstrand	IT	Operating	information	data quality
Response 2	in	its	Security	in terms of	where	print	security	runs	software	which	communicatic	virtually	access	a	The	the	Security	Operational	a	implementati
Response 3	in	high	certain	all	system	social	IT	like	telephonic tra	in which	Biometrics	telephonic	people	neccesary	firstrand	fnb	security	the	secured	only
Response 4	in	the	Information Security	irrespective	the condition	electronically	information	applications	manual proce	means of how	manual	or other relev	access to evei	a	The Informati	FRG (First Rar	Management	IT Informatior	a Risk	overall / grou
Response 5	in	information	Control	irrespective	which	digital	information	electronically	applications	which	transmission	paper	access	a	The	the	Risk	Information	the	organisationa
Response 6	in	high	Preventative	Some	How	External	Application	OS	databases	Which	Devices	Cloud	Transfer	A	Group	The	Tool	IT	The	Complete
Response 7	in	it's	strict	type	which	electronic	computer	thoroughly	etc	which	message	etc	access	a	This	the	systems	Information	a	continued
Response 8	in	it's	Control	for protectior	where	electronic	information	for example	processing	which	digital	telephonic	access	the	Information s	an	and IT	IT	a key	organisationa
Response 9	in	utter	These	always	confidential	removable	information	further	storages	which	devices	manual	access	a	the	specific	security	IT	a	security
Response 10	in	high	Security	in light	where	social	Operational	electronically	etc	which	systems	Telephonicall	access	a	Information s	the	security	Operational	a useful	guaranteed
Response 11	in	its	Adequate	relevant	which	social	Electronic	digitally	physical	which	platforms	physically	access	the	Access	the	Security	Information	a	continued
Response 12	in	its	Security	regardless	which	electronic	the	computers	etc.	which	mail	etc.	access	the	The	FirstRand	Technology	Enterprise	a	business
Response 13	in	extreme	all	free	how	social	computer	uses	etc	how	systems	email	public	the	information	the	security	the	a	continued
Response 14	in	its	Security	regardless	which	multi (electro	the	computers	etc	which	mail	etc	access	the	This	the	Technology	Enterprise	a	business
Response 15	in	the	Control	irrespective	which	electronic	The	Computers	etc	which	mail	etc.	access	the	the	an	technology	Enterprise	the	our
Response 16	in	its	Security	on which	which	electronic	the	systems	etc	which	media	etc	access	the	The	FirstRand	Technology	Enterprise	a	business
Response 17	in	Information	appropriate	across the ha	which	electronic	information	content	etc.	which	media	etc.	access	the	The	the	security	Enterprise	a	business
Response 18	in	its	Security	Regardless	which	electronic	the	computers	ect	which	mail	ect	access	on	this	the	Technology	Enterprise	a	business
Response 19	in	privacy	security	when making	which	multi	technology sy	such as	and other sys	which	mail	paper based (	access	user	information s	the	information s	information	risk	its
Response 20	in	the	adeqaute	in terms	the	Electronic	Information	ongoing	etc	which	?	etc	access	required	this	the	security	the	adeqaute	the
Response 21	in	the	security	regardless	which	electronic	IT	automatically	etc	which	mail	etc	access	strict	this	the	technology	enterprise	a	business
Response 22	in	the	Stringent	in the manag	which	digital	communicatic	?	?	?	communicatic	?	access	the	This	FirstRand	security	IT	a	compliance
Response 23	in	the	the	ahead	where	electronic	Computer	anyways	etc	which	ally	etc	access	purely	Information S	the	Security	Information	Control	complete
Response 24	at all times ir	regulation wh	Stringent	with consider	all devices wh	mobile device	digital	not sure	not sure	how	transfer	paper	visibility	not sure	Group	not sure	Security	not sure	necessary	not sure
Response 25	In	the	Practical	despite	where	systems	application	devices	etc	which	messages	etc	access	the	the	an	security	Effective	risk	security
Response 26	in	the	Security	irrespective	which	digital	application	daily	not sure	which	mail	digital messa	access	business/user	The	FirstRand	Security	FirstRand	a	regulatory
Response 27	in	accuracy	security	n/a	personal	applcation	2	outlook	5	look	into	why	and	Because	Will	Events	Customise	introduce	be	a
Response 28	and secured i	high	safety	to prevent ac	where	Electronic	secured by	and present i	applications	presenting	media	or on app	access	customer	This	the	to	company and	the only	total
Response 29	in	high	strong	storing	confidential	digital	electronic	electronically	email	paper	interface	in-person	access	the	security	FirstRand	Security	effective	a	continued
Response 30	in	its	Security	regardless	which	electronic	the	computers	etc	which	mail	etc	access	the	This	FirstRand	Technology	Enterprise	a	business
Response 31	in	the	security	the	security	information	IT	the	email	electronic	devices	paper	access	the	The	FirstRand	management	IT	the	governance
Response 32	securely	its	Security	irrespective	which	digital	information	securely	etc.	which	format	or otherwise	sharing	a	Data Protecti	FirstRand Gro	System	Information	its	its
Response 33	in	it's	Security	regardless	which	electronic	the	computers	etc	which	mail	etc	access	This	security	the	technology	Enterprise	a	business
Response 34	in	adequate	Appropriate	regardless	which	digital	by	automatically	etc	access	user	The	FirstRand	Security	IT	the	security	security	the	Security
Response 35	in	it's	Appropriate	(?)	where	electronic	tecnical	electronically	etc	where	mail	etc	access	the	this	the	technology	integrated	a	business
Response 36	in	the	Adequate	to use	where	social	all	daily	written	social media	written	oral	access	relevant	security	all	security	security	preferred	overall
Response 37	with	all	n/a	n/a	n/a	less	any	must	n/a	which	n/a	n/a	all	only	privacy	the	security	the	important	all
Response 38	in	its	Security	regardless	which	electronic	the	computers	etc	which	mail	etc	access	the	The	the	Technology	Enterprise	a	business
Response 39	in	its	Security	regardless	which	electronic	the	computers	etc	which	mail	etc	access	the	This	Firstrand	Technology	Enterprise	a	business
Response 40	in	its	all	Protection	record	email	IT	like	storage	which	media	emails	access	a	This	security	security	information	a	overall
Response 41	in	its	Security	regardless	which	electronic	the	computers	etc	which	mail	etc	access	the	data privacy	firstrand	technology	enterprise	a	business
Response 42	in	information	Security	regardless	which	electronic	including	follows	databases	which	processes	paper-based	access	purpose	IT Security	mandated	security	IT	mandated	regulatory
Response 43	in	utmost	Security	to all	when	hard	banking	applications	mail	which	transport	physically	Access	the	This	holding	Security	Information	our	compliance
Response 44	in	high	Stringent	across all	which	digital	information	internally	telephones	which	communicatic	written comn	access	the	Information S	an	Technology	Information	a critical	continued
Response 45	in	its	Security	regardless	which	electronic	the	computers	etc	which	mail	etc	access	the	This	the	Technology	Enterprise	a	business
Response 46	always	level	Control	Measuring	which	email	IT	computers	servers	which	postal	telephone	access	level	Information	LRC	Solutions	Data	organisationa	system
Correct word	in	its	security	regardless	which	electronic	the	computers	etc	which	mail	etc	access	the	This	FirstRand	Technology	Enterprise	a	business
Countifcorrect	38	17	19	12	24	20	9	10	19	28	13	14	36	20	12	10	13	10	22	11
Percentage cor	82,6	37,0	41,3	26,1	52,2	43,5	19,6	21,7	41,3	60,9	28,3	30,4	78,3	43,5	26,1	21,7	28,3	21,7	47,8	23,9

Word Deleted	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Response 1	important	data	controls	operations	ensure	framework	assess	entity	regular	critical	control	are	confidentialit	using	data	confidentialit	needs	remains	granting perr	information
Response 2	managed	security	processes	guidelines	be	specific	review	the	regular	security	the	are	restriction	allowed	defines	dependability	it	making	receipt	Security
Response 3	well known	risk	policy	data	be	consulted and	be aware	to	monthly	important	sensitive	is	nature	intented	safety	source	protection	information	verification	privacy
Response 4	administered	and Security	policies	processes	become	Information S	review	to the	regular	Information a	the	occurs	viewing	who is entitle	ensuring	relevancy	time	ensuring data	the time	The Informati
Response 5	implemented	Security	policies	procedures	become	security	review	to	regular	security	the	are	restriction	authorised	ensuring	completeness	it	being	request	The
Response 6	Correct	Tool	Processes	Policies	be	Policies	familiarise	to the	Monthly	Types	Risk	Is	Privacy	Available	Security	Privacy	IT	Organizations	Reliable	Group
Response 7	accessed	Security	policies	guidelines	be	annual	review	to	Regular	access	the	are	protection	authorised	ensures	validity	it	data	request	the
Response 8	managed	Security	policies	processes	ensure they a	ISMS	review	to the	annual	main	the	are	privacy	authorised	validity	security	of data	management	valid	Information s
Response 9	managed	Security	law	policies	be	information	review	to	annual	main	the	are	sharing	authorised	the	integrity	data	data	access	The
Response 10	circulated	security	to	procedures	be	policies	capture	into	regular	security	IT	is stated	privacy	permitted	is	consistency	data	data	request	Security
Response 11	operationalis	Security	processes	procedures	be	Risk	review	to	regular	basic	Management	are	restriction	required	maintain	correctness	thereof	data	approval	The
Response 12	managed	Security	strategies	controls	be	FirstRand ISM	review	to	quarterly	security	the	are	restriction	authorised	Safeguarding	completeness	methods	being	demand	This
Response 13	conveyed	policy	policies	procedures	be	stipluated	comply	to	daily	main	the	are	protection	authorized	is	consistency	methods	how	request	Security
Response 14	managed	security	strategies	controls	Each	ISMS	review	to	quarterly	security	the	is	restriction	authorised	safeguarding	completeness	methods	being	demand	The
Response 15	managed	security	governance	methodologie	become	own	review	to	quarterly	security	the	are	restriction	authorised	Protecting	completeness	methods	First Rand	demand	The
Response 16	managed	security	objectives	governance	be	policies	review	to	regular	security	the	are	restriction	authorised	Securing	completeness	tools	bring	demand	This
Response 17	managed	Security	policies	objectives	be	required	review	to	regular	secuirty	the	are	protection	who are requ	protecting	validity	integrity	information b	request	The informati
Response 18	managed	security	strategies	controls	be	structures	review	to	quarterly	security	the	follows	restriction	authorised	safeguard	completeness	methods	being	demand	This
Response 19	managed	security	policies	frameworks	become	information s	embed	to	ongoing	risk	the	may be listed	availability	authorized	testing	integrity	controls	making inforr	request	The Group's I
Response 20	embeded	access	the	to	able	not	be	too	yearly	3	the	are	privacy	who	integrity	ability	data	on	end	information
Response 21	executed	security	policies	reporting	be	defined	review	to	regular	crticical	key	are	securing	able	ensure	integrity	thereof	being	request	the
Response 22	implemented	security	protocols	guidelines	be	IT Security Ri	implement	to	monthly	cirtical	the	is	access	who	the	usefulness	?	the	analysis	The Informati
Response 23	Implemented	security	Protocol	Implementati	be	Information	follow	to the	regular	types of	An Organizati	are	sharing	who need	Validate	Storing	Accurately	the data bein	requested	Information S
Response 24	pervasive	not sure	guidelines	rules	become	not sure	not sure	not sure	not sure	principles whi	group	not sure	security	who need	not sure	not sure	not sure	information	receipt	the Informati
Response 25	managed	security	guidelines	best practice	be	review	information s	with	periodic	main	key	are	provision	authorised	ensuring	completeness	methods	being	access	Information s
Response 26	driven	Security	to	procedures	be	not sure	adhere	to	annual	key	the	are	access	allowed	ensure	not sure	not sure	information	receipt	FirstRand
Response 27	and	a	be	and	why	because	ok	aware	initiate	testing	ISMS	are	is	when	to	completeness	information	infomration	media	no
Response 28	governed	risk	procedures	policies	be	processes	protect	to	Regular	risk	protection of	are governed	access	authorized	presenting	protection	rules	Firstrand Ban	Request	Risk
Response 29	managed	Security	policies	guidelines	become	Security	review	to	Annully	security	FirstRand's	are	restriction	authorised	safeguarding	completeness	methadology	being	demand	The
Response 30	managed	Security	strategies	controls	be	FirstRand ISM	review	to	quarterly	security	the	are	restriction	authorised	Safeguarding	completeness	methods	being	demand	this
Response 31	managed	security	policies	governance	get	official	review	to	regular	recognised	all	are	the	ask	trust	management	data	information	approval	Information
Response 32	managed	Technology	protocols	rules	become	particular	implement	to its	yearly	main	Management	are	limitation	required	maintaining	completeness	quality	FirstRand	request	Information S
Response 33	managed	security	strategies	controls	be	isms	review	to	quarterly	security	the	are	restriction	authorised	safeguarding	completeness	methods	being	demand	This
Response 34	managed	security	frameworks	policies	be	applicable	review	to	annual	main	the	are	visibility	require	relates	validity	speeed	data	access	The
Response 35	managed	security	policies	procedures	be	ISMS	review	the	regular	technology	the	are	restriction	need	ensuring	authenticity	data	ensuring	request	This
Response 36	governed	secuirty	procedures	policies	be	defined	review	to	regular	security	the	are	use	who	the	use	data	FirstRand	business	The security
Response 37	based	security	to all	ensure they	policies	ensure	n/a	to the	ongoing	policy	all	reads	access	authorized	requires	privacy	n/a	information	n/a	the
Response 38	managed	Security	strategies	controls	be	ISMS	review	to	quarterly	security	the	are	restriction	authorised	Safeguarding	completeness	methods	being	demand	This
Response 39	managed	Security	strategies	controls	be	ISMS	review	to	quarterly	security	the	are	restriction	authorised	Safeguarding	completeness	methods	being	demand	This
Response 40	managed	security	systems	architecture	be	policy	read	to	regular	information	the	are	belonging	who	managing	reliability	requirements	data	authorisation	This
Response 41	managed	security	strategies	controls	be	Firstrand ISM	review	to	quarterly	security	the	are	restriction	authorised	safegaurding	completeness	methods	being	demand	this
Response 42	managed	security	regulations	standards	be	defined	monitor	established	regular	principal	govern	are defined	presentation	authorised	ensuring	use	data	readily	approval	IT Security
Response 43	managed	security	policies	more	be	internal	action	on	recurring	primary	the	are	limiting	meant	Ensure	trustworthine	thereof	publicly	confirmation	This
Response 44	controlled	Technology	policies	procedures	become	existing	share	to	regular	critical	all	are	Privacy	who	covering	correctness	guidelines	the organisat	access	This
Response 45	managed	Security	strategies	controls	be	ISMS	review	to	quarterly	security	the	are	restriction	authorised	safeguarding	completeness	methods	being	demand	This
Response 46	diverse	enterprise	controls	measures	ensure	team	read	owner	adhoc	main	Group	are	protection	able	with	reading	storing	customers	registered	Information
Correct word	managed	Security	strategies	controls	be	ISMS	review	to	quarterly	security	the	are	Restriction	authorised	safeguarding	completeness	methods	being	demand	This
Countifcorrect	23	29	8	9	30	7	24	26	8	15	26	34	14	17	8	15	12	12	12	13
Percentage cor	50,0	63,0	17,4	19,6	65,2	15,2	52,2	56,5	17,4	32,6	56,5	73,9	30,4	37,0	17,4	32,6	26,1	26,1	26,1	28,3

Word Deleted	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55
Response 1	employees	external	and	is	infustructure	firstrand	data	AI	computer	to-end	policy	other	that	need	adequate
Response 2	employees	as	and	is	processes	the	its	information	systems	users	policy	associated	by	systems	and
Response 3	members	as	and	is also	systems	various	many	security	sensitive info	result	data	firstrand	when	in order	should
Response 4	employees	as	and	is	processes	First Rand	its	cloud	mainframe	users	policy	adherence to	and	required	and
Response 5	employees	as	and	is	process	the	information	cloud	mainframe	users	policy	security	when	systems	and
Response 6	Users	as	Vendors	is	and	control	Risk	which is	Risk	users	Policies	Risk	provided	Risk	To
Response 7	employees	as	and	is	systems	the	data	electronically	systems	users	rule	implemented	when	and	to
Response 8	employees	external	and	is	process	the	information	cloud	networks	users	policy	other relevar	when	assets and sy	and to
Response 9	personnel	as	to	is	processes	the	data	the	systems	users	policy	related	for	sources	and
Response 10	areas	independent	and	is	systems	the	the	cloud	systems	user	policy	security	of	polocies	and
Response 11	staff	external	and	is	processes	the	its	information	systems	state	policy	other	by	policy	and
Response 12	employees	as	and	is	process	the	data	cloud	system	users	policy	related	when	resources	and
Response 13	employees	to	and	is	process	the	its	software	and	users	policy	relevant	when	system	to
Response 14	employees	as	and	is	processes	the	data	cloud	systems	users	policy	related	when	resources	and
Response 15	employees	as	and	is	systems	the	all	cloud	systems	users	policy	group	when	so	and
Response 16	empolyees	as	and	is	processes	the	data	cloud	systems	users	policy	applicable	when	resources	and
Response 17	employees	as	and	is	processes	the	system	cloud	information	users	policy	related	when	systems	and
Response 18	employees	as	and	is	processes	the	data	cloud	systems	users	policy	related	when	resources	and
Response 19	employees	casual	and	is	processes	the	group	?	?	user	policy	group's	when	in order to	and
Response 20	the	temperory	and	is	process	the	IT	cloud	offsite	user	requirement	stndards	this	is	to
Response 21	employees	external	and	is	processes	the	information	cloud	access	users	policy	related	when	systems	and
Response 22	employees	as	and	is	systems	the	its	cloud	?	End users	policy	related	when	?	and
Response 23	employees	as	vendors	is	systems	the	other	server	processes	point	policy	policies	which are	in order	and
Response 24	employees	as	not sure	is	not sure	the	not sure	not sure	not sure	not sure	not sure	not sure	not sure	not sure	not sure
Response 25	employees	temporary	and	is	processes	the	information	vendor	systems	user	policy	applicable	when	assets	and
Response 26	members	as	and	is	process	FirstRand	data	not sure	systems	users	standard	Security	not sure	not sure	availability
Response 27	to	yes	no	because	if	how	they	information	data	compelte	accurate	data	why	if	and
Response 28	employees	as independa	companies an	is	processes	FRG's	data	mainframe	off host	Users	Processes	risk	when	data	and
Response 29	employees	as	and	is	process	the	its	cloud	cloud	end	policy	ancilliary	when	and	and
Response 30	employees	as	and	is	processes	the	data	cloud	systems	users	policy	related	when	resources	and
Response 31	Governance	as	vendors	is	business	the	organisations	cloud	network	user	policy	group	legislation	system	issues
Response 32	employees	independent	and	is	systems	FirstRand	its	Internally	systems	users	system	Group's	when	in order	and to
Response 33	employees	as	their	is	processes	the	data	cloud	systems	users	policy	related	when	resources	and
Response 34	areas	as	and	is	process	the	the	cloud	systems	state	policy	relevant	that	security	and
Response 35	employees	permenent	and	is	systems	the	information	cloud	systems	users	policy	related	that	systems	of data
Response 36	businesses	as	of	is	vendors	the	secure	FirstRand's	websites	user	policy	security	when	and	and
Response 37	employees	as	and	applies	employees	fsr	policy	n/a	n/a	users	policies	privacy	n/a	n/a	n/a
Response 38	employees	as	and	is	processes	the	data	cloud	systems	Users	policy	related	when	resources	and
Response 39	employees	as	and	is	processes	the	data	cloud	systems	users	Policy	related	when	systems	and
Response 40	employees	as	their	is	systems	the	information	its	systems	users	policy	security	and	adequately	to
Response 41	employees	as	and	is	processes	the	data	cloud	systems	users	policy	related	when	resources	and
Response 42	employees	as	entities	is	systems	data and	other	system	information	users	regulations	IT	including	resources	thereby
Response 43	management	External	including	is	processes	the	all	cloud	databases	systems	document	company	actively	strategy	to
Response 44	employees	as	and	is	systems	the	their	locally	systems	users	policy	other	by	systems	and
Response 45	employees	as	and	is	processes	the	data	cloud	systems	Users	policy	related	when	resources	and
Response 46	levels	sub	and	can	machines	work	education	Industrial rel	processing	users	policy	standards	framework	use	measurment
Correct word	employees	as	and	is	processes	the	data	cloud	systems	Users	policy	related	when	resources	and
Countifcorrect	31	30	32	42	19	33	15	22	21	29	34	13	25	9	29
Percentage cor	67,4	65,2	69,6	91,3	41,3	71,7	32,6	47,8	45,7	63,0	73,9	28,3	54,3	19,6	63,0

Appendix 9: Interview Transcripts
Transcript 1

Researcher: Participation in the study is completely voluntary. So you're not under any pressure, any duress by your line manager, anyone at [redacted], or myself to participate. And then secondly, I need to inform you that your responses are treated confidentially and with the utmost of privacy, and none of your responses will be shared with your line manager or would be used to individually identify you as part of the study and then. Uh, sort of. Lastly is to inform you that you know this this study is. Conducted in my individual capacity, so I'm trying to understand how information security policies are embedded, rolled out, understood and then applied within the organization and part of the study requires me to conduct some interviews, this being one of them. And are you comfortable to proceed?

Interviewee: I'm comfortable all in order.

Researcher: OK, so there are seven questions for you to answer. These are open-ended questions. So they really are entirely up to you in terms of how long or how short the answers can be. So I'm not going to interrupt you when you are speaking.

Interviewee: OK.

Researcher: OK. Question number one. Could you briefly describe IT security to me?

Interviewee: So when I think of IT security, I think of protecting information and more specifically the processing of information. And then also just to ensure that systems? Up and running with regards to. An authorised parties that may have information or may have access to IT security. So in my mind that is what I think it might be.

Researcher: OK. Question number two, what role does IT security policy so the emphasis is on policy? What role does IT security policy play in keeping an organization safe from threats?

Interviewee: I should think that the regular audits would be performed to ensure that security practices are compliant at all time and also just. To monitor the networks. And if there are any irregularities that. That is picked up as soon as possible. And then also just to ensure that. These access controls. As well as access management systems. That's what I would say.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: I would think they are. I don't think I've ever had an experience way by they were inadequate. So I would say yes.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Oh my word it's the same like when a client calls into stockbroking and they ask us about corporate actions and they cannot understand. So I would think that if they were jargon that was used, you know there's always synonyms that one can use when you use a specific. A specific word and it might not resonate with everyone. So I think the jargon. You should be my someplace. So instead of also using acronyms, just simplify that and use the full name. But however, just use plain simple English that everybody can understand because I know I get very confused when I speak to an IT person and I'm like oh you just lost me

there. I don't know what you're saying. Are you speaking another language? So just to simplify the language? I think we'll make a difference.

Researcher: OK, if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: Improved I think. When IT roll out processes or they involved in certain incidents that may have been raised, if they could, maybe. Give analogies way by. It makes a lot more sense where people are familiar with what they are saying as well as visual presentations. And then after the presentation, maybe a quiz. I think that will give everyone an understanding of what was just being presented.

Researcher: OK. In your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: No, I know I don't know much about IT, so I think you guys are doing a good job.

Researcher: OK. And then lastly, where would you locate our information security policy?

Interviewee: You know what you got me there. Please tell me so that I can save it.

Transcript 2

Researcher: To inform you that your participation in the study is 100% voluntary, so you're not under any pressure by your line manager, myself or anyone else to to participate. And then secondly, I need to inform you that the responses that you provide here this afternoon will be treated confidentially. They're not going to be shared with your line manager. Anyone at [redacted] Or used to uniquely identify you. Are you comfortable to proceed?

Interviewee: OK. I am.

Researcher: OK, so the format of the interview this afternoon, there are seven open-ended questions that I need to ask you and because they are open-ended, there's no limit on how long short your responses can, should or would be. So I'm not going to interrupt you when you're speaking so that you can finish answering. Are you ready to go ahead?

Interviewee: Yes, I am.

Researcher: OK. So question number one, could you briefly describe IT security to me?

Interviewee: I information security. I believe that that might be with regards to. Information and how we protect the client or our personal information.

Researcher: OK, what role does IT security policies? I'm specifically asking around security policy. What role does IT security policy play in keeping an organization safe from threats?

Interviewee: So the role that they play is making sure that the information is not misused and prevents this information from being used against the clients or maybe getting into people or acres ends and being used against them for malicious purposes.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Umm yes, I would believe that we do have. Policies we please that is like working to keep clients information and our personal information safe. So it will be it does work, yes.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Umm do you mind clarifying that question?

Researcher: So IT security policies sometimes not always, but sometimes they do tend to have lots of abbreviations and technical terms. How should they be improved or simplified in your opinion?

Interviewee: On my side, I think we can maybe like make it easier to understand by. Making like for instance knowledge sessions where we can like understand the information policies much better like in my cases, I would believe that using larger words and all of the terminologies is quite hard to understand and to remember. So making it easier to understand and read will make it easier to like for us to understand the policies altogether. So making it just simpler. You know, like maybe some. drawings, or maybe some. Smaller words, or maybe some? Abbreviate and I'm what you call this words. The shorten words like lol or something like that where we can use it much easier, you know.

Researcher: OK, If IT security awareness specifically could be improved, what would that entail in your opinion? So specifically the awareness piece I'm asking about so IT security awareness could be improved. What would that entail in your opinion?

Interviewee: Well, it will make things much easier for all of us, because then we'll be aware of all of this and security information that we need to be aware of. And which will make us much more knowledgeable when it comes to these type of conversations. So it will be easier to understand for all of us, you know, if I'm on my side, I think I'm not quite familiar with the ITC policies altogether. So if yeah, I could have been like maybe some training sessions or maybe some. Banners or maybe some emails, or maybe some information relating to more of this, like in a funnier or maybe in an entertaining way. Or maybe something like that which would like make better. Awareness for all of us, for me as well, and I would have understood the project a little bit better.

Researcher: OK. And in your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Not that I'm aware of now.

Researcher: OK. And then the last question was said of where would you locate our information security policy?

Interviewee: On [redacted]

Transcript 3

Researcher: So thanks for joining me this afternoon. So I am required to inform you, that your participation in the study is 100% voluntary. You're not under any pressure from your line manager, myself or anyone to participate. So if you would like not to proceed, you're welcome to say so. And then the second thing that I need to inform you is that your information, your responses are treated confidentially. None of the information or responses that you provide to me will be shared with your line manager, anyone at [redacted] or used to uniquely identify you. Or to to pick you out. Are you comfortable to proceed?

Interviewee: OK. Please proceeds.

Researcher: OK, so the nature of the interview this afternoon, there are seven open-ended questions for me to ask you. They are open-ended, so there's no limit on how long or short the responses can, will or should be. I will not interrupt you when you are speaking or answering so as not to cut your answers short prematurely. Are you ready to go ahead?

Interviewee: OK. No problem. We can go ahead, yes.

Researcher: OK. Question number one. Could you briefly describe IT security to me?

Interviewee: IT security. OK. All right. So IT security in my own understanding is when it has to do with information that has to do with whatever is that we're dealing with in terms of data that includes clients, personal information, that is very important that that is a secured with everything. In terms of the POPI, I don't know if it makes sense. I'll just make an example on my side. So I normally deal with momentum queries, so momentum is taken as a third party whereby we then correspond regarding clients documents, so I'm liable for sending documents to momentum. So in that case, there's what there's what we call a zip file whereby I normally zip the files and then send them to momentum and then reshare a certain standard password with momentum. For them to then make sure that they receive the file and. They they basically received the file, Umm securely. Even on our side, we know that the files are received saved safe. Umm to momentum at UMI? Don't know if it makes sense, so that's basically my understanding. Yes we need to make sure that all the documents or whatever data is secured or whatever information is secured.

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: Right. So mostly I would like to include what we call the cyber security whereby it is very important that the IT security protects all of those in terms of the boundaries on but ever that may affect the. The system of the company to threats from outside of people or cyber. That are trying to like try to maybe access the the the system of the company and in in terms of maybe theft or whatever the case may be, that can be a danger to to the business and to our clients as well.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Yes, certainly there are very adequate with all the systems that I see that is are are used in terms of securing the data that is within the organization including what we mostly deal with, which is our clients. Personal information regarding the POPI Act.

Researcher: OK and the use of jargon and technical terms is common in such policies.

Interviewee: Jargon?

Researcher: How should they be improved or simplified? Yes, jargon in the sense of technical terms, abbreviations. You know non standard terms, they are common, not always necessarily, that ou will find them in every single policy, but in IT security policies you would sometimes find them and in your opinion how should they be improved or simplified.

Interviewee: OK. So in terms of them being simplified sometimes as a as the agents, so I'll make an example with myself. I work in a call center agent whereby we we use numerous types of systems. So sometimes it happens that whatever system that is placed on maybe online whereby on our side we normally use online. I share accounts are normally based on line, so the clients would open them there. So most of the data or information that is placed

there is not what we can. Actually, it's not what it's easily accessible on our side, so it gives us a bit of a problem now because the client would come and complain. So this is what I'm seeing. This is not what is happening and I want this or to do this online regarding my account and then on most of the time we always have to ask them to send screenshots on our side for them For us to see what they're seeing, because we cannot access up to date. We cannot access that, that system that they have on their end and it becomes a bit difficult to us to assist the client. So sometimes we I would like to maybe just add that maybe the IT team can maybe just try to maybe just break it down for us so that whatever access the client or whatever system the client can access online, we also have the very same processor on our side so that it's easier for us to assist the clients on our end.

Researcher: OK, if IT security awareness could be improved, what would that entail in your opinion?

Interviewee: OK. So it would entail that. Like I said Umm, previously it would improve more on our side in terms of the skill to assist the clients and then just accelerate or provide clients with good customer service in terms of as like in terms of how we can assist the clients and make it easier for them and for us to give them a better client service experience basically.

Researcher: OK. And in your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: OK. Umm yes, I haven't thought of 1 now, but it's basically going back to what I mentioned earlier that I wish that the IT three securities can maybe just try to break down the systems for us on our side so that we can easily be able to to to assist our clients for us to give them better client service. So it's basically that on my side. I may not know. How it can be done? But I know that it's a doable process. I'm I'm I don't know if I'm making scenes.

Researcher: So so I'm trying to understand, do you do you think that they are adequate opportunities for your input or your views around IT security?

Interviewee: Yes.

Researcher: To be incorporated, so are they adequate avenues available to you to provide that information to someone in the organization, specifically around IT security and then for them to take that into account?

Interviewee: Yes, yes, yes, definitely. I'm not sure if I'm understanding your your question. Can you maybe just rephrase it and maybe ask it in a different way maybe?

Researcher: Sure, so within the organization, IT security policies basically are published and employees are required to not only read them, but also to act on them. So if there's anything that you are required to do or be aware of in a policy, the fact that you have read the policy means that you understand what's required from you. So my question is if there was something you were unhappy about or you would like changed around IT security.

Are there adequate opportunities for you to provide that information or for that feedback from you to be given?

Interviewee: Definitely they are so also make an example for me to be able to put it in picture. Or in images in my mind. So we have what we call an IP and access. So that was recently launched or introduced to us for us to to improve the clients verification and security around the data, right. So with regards to app and most of the time Appian is very slow. So that affects the, the. The the the customer experience in a way that normally the call if the

call will take 2 minutes on the call, now takes about five to six minutes and the clients would start complaining. But why? Why are we now doing this? Because before you guys would verify us manually whereby we would just tell you information and then you verify us telephonically as the calls are recorded right for quality and security purposes. So why do we now have to go through this process? We buy you guys have to send out that notification on the app and it gets complicated if I'm somewhere that there's no network that I can actually access my [redacted] app and I can not receive that verification and then it becomes a problem because I will then have to go to the nearest branch and then be verified there, which it's a long process for me to get my funds before it was like an immediate process. So I think maybe that's what I could I I would forward would suggest that it's maybe changed in terms of verification wise. Can can can that maybe be changed in a way that can be? Not really simplified, but that can be. That can be done in a way that will make the clients happy in a way, and for us to not be also frustrated because now if the clients are frustrated, we also become frustrated as most of the time whatever happens with the system is not on our hands, but it's on the IT side. And then again the second option is sometimes it happens that the systems are down, the app is down and we get a lot of complaints as we are on the. Basically are on the front frontline, so whatever happens, the clients call us and we have to then explain what we don't really know what's happening. If if the app is down or if online banking is down, the clients cannot place trades and the now missing out in the share prices or whatever the case may be, it hits US hard on our side because it's out of our control and there's nothing else we can do to assist the clients. And then we get to have a lot of complaints and sometimes we even tend to lose the clients because of that.

Transcript 4

Researcher: So I just need to inform you that your participation in the study is completely voluntary, so you're not forced to participate and we can end the interview at any point in time. Your responses are treated confidentially, so we don't share your information with line managers or with anyone else, including the bank. Are you comfortable to proceed?

Interviewee: Yes

Researcher: OK, so the format of the questionnaire basically it's just a question and answer. So I ask you the question and you you respond with the answers, Are you ready to go?

Interviewee: Yes

Researcher: OK. So question number one, could you briefly describe IT security to me?

Interviewee: IT security is about safety within the company like like VPN I need to if I'm working from home I need to log in through VPN to make sure that the the information of the company is not exposed to the wrong devices or the wrong people.

Researcher: OK, what role does IT security policy playing in keeping an organization safe from threats?

Interviewee: Well, I think the US systems or check lines that are installed on our on our laptop to make sure that the information is not exposed.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Yes, I do.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Can you simplify the question?

Researcher: So so basically I just security policies, they tend to have like most other policies that you would find in, in, in, in, in any organization, they tend to have lots of acronyms and abbreviations. So these acronyms and abbreviations which are which are fairly common, how should they be improved or simplified?

Interviewee: Ohh, I think they can use a simpler terms picture or like picture or maybe pictures just to simplify.
Like for me, I just ask you can't you simplify your question just for the message to be passed through easily? They can use simpler terms or pictures.

Researcher: OK, if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: So. Uh. Well, they don't. They don't have to put so much measures like.
For me to access [redacted] facilities man, they just need to be simplified.

Researcher: OK. In your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: You mean, in my own opinion?

Researcher: Yeah.

Interviewee: Yeah, I think there is.

Researcher: OK. And where would you locate our information security policy?

Interviewee: Uh online, [redacted] think I think our website.

Transcript 5

Researcher: So thank you so much for agreeing to participate in the study.

Interviewee: OK.

Researcher: Basically the format is basically just question and answers, so it's up to you and I'm required to inform you that your participation in the study is completely voluntary, so you are not under any pressure at any point in time. If you're not comfortable with the questions, you can indicate and we can end the interview.

Interviewee: OK.

Researcher: And also none of your information will be used to personally identify you and none of your responses also will be shared with the research organization or will be shared with line manager. So your responses to the survey are completely confidential. Are you comfortable to proceed?

Interviewee: OK. I see. Yes, thank you.

Researcher: OK. So the first question is, could you briefly briefly describe IT security to me?

Interviewee: IT security, OK. As far as I know, it's more about. No man, I'm not 100% sure now it's more about. They it like more about the virtual, what you call the virtual world, we in you know I'm not too sure. I don't want to lie to you.

Researcher: OK, OK. What role does IT security policy play in keeping an organization safe from threats?

Interviewee: Umm. OK, I think it's more for. Information you know the protection of the information and mainly the client information going out there.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Yes, yes. Because we always run the we always do the assessments and they make sure that we are aware of the bridge that might be you know in, in just in case we are to fall into the trap of kind of sharing too much or yeah. Something like I've done.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Umm. OK, it's common. Sorry, I don't think I understand. Let's let's do the question again. Sorry.

Researcher: So the use of jargon and technical terms in is common in such policies IT security policies. How should they be improved or simplified?

Interviewee: OK. Maybe the abbreviation shouldn't be too? How can I say it shouldn't be too technical, it should be kind of user friendly way.
Everyone and anyone is able to understand what is being said, or maybe with the abbreviations then there should be like longer versions of it.

Researcher: OK, if I IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: Alright, Jesus. Thank you. It OK. Um. I think it would be more user friendly. OK that everyone is able to understand. And I think it should be simplified.

Researcher: OK, in your opinion, are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Yes, I think with more awareness and also the kind of meetings that we have in like this one where we it's not just part of assessments that we are to do, you know and it it should be more I wouldn't really say personal, but like more with the is personal contact that we are to be familiarized with the matters. We mustn't just push because within working hours I'm going to be very honest with you. Sometimes when we do that ITC assessment or whatever you're doing it just to go through it and to pass it. And you're like, yeah, yeah, yeah. You kind of know the confidentiality clauses, what you're supposed to do and what you're not supposed to do, but you you kind of run through the material. So if there was maybe time sort of accommodated like we're doing now. Where we can have those sessions and it be more personal and yeah, it would be more. It will be more well known and it would be practical than as having it as theory, so to speak.

Researcher: OK. Thank you. Where would you locate our information security policy?

Interviewee: Located on our sharepoint we this information and there's various websites that [redacted]usually offer OK, but we don't usually access it or ever really know 100% where to go. But when we supposed to do it we always notified and then we go into it, yeah.

Transcript 6

Researcher: Your participation in this study is voluntary Or would line managers and your your responses to the questions are also anonymous, so you will not be, you know, uniquely identified via your responses.

Interviewee: OK, alright. Is it hard?

Researcher: Are you comfortable? So it's basically just questions. I ask you the questions you answer them, that's it. They're just seven questions. OK, so.

Interviewee: Ohh, that's a lot, but OK.

Researcher: The first, uh. The first question is, could you briefly describe IT security to me?

Interviewee: It's. OK, I suppose it is protecting information from unauthorized use or unauthorized access so. Basically mitigating the risk of unauthorized access tube information.

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: What role do they play like? Well, like I mentioned earlier, trying to protect the information basically by informing us on how to do so, providing us with training and steps on to what to do if. Any security breach has happened and so forth. Do you think?

Researcher: OK. Thank you. Do you believe our organizational IT security policies are adequate?

Interviewee: Yes, I do.

Researcher: Can you tell me the use of jargon And technical terms is common in policies. How should they be improved or simplified?

Interviewee: Trying to use less jargon I suppose make it more understandable to us, like explain things in layman layman's terms, something that we can understand instead of using words we don't understand, because when I come across the word I don't understand, I just get blank. So maybe if you're using simple English it's much easier and more.
Explainable to us, you know?

Researcher: OK, if I IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: Maybe more awareness, more emails sent to us to raise the awareness, maybe more surveys or. Obviously we get the training, so I can't say about that. So maybe more awareness in terms of sending us pop up emails or maybe? Some surveys. To get a small when to create more awareness. Yeah, that's what I think.

Researcher: OK, in your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: I think they are. I believe they are because I mean we we get the tests all the time that we need to undergo. But The thing is we only get to know about it when we get those tests that we have to do and we told OK, you need to do it by this time. So if we if we don't. Get that? Then we practically don't get any more information. So like, it goes back to what I said about awareness, maybe some more informative emails just to let us know, because if you don't go digging, then you really don't know the info. So I mean, if I don't go in the Internet and I hardly get the time to because it's always busy if I don't go in the Internet to look for more info, then I probably wouldn't know if I didn't get those tests. So maybe on the lighter side. Nice emails that will be sent to just inform us doesn't have to be a lot of information. Maybe like one e-mail per week. Uh, focusing on one aspect and then. And next month may be focusing on another aspect, you know.

Researcher: OK, And where would you locate our information security policy?

Interviewee: Yeah. And I'd have to wait on the Intranet like I've mentioned on the [redacted] Internet or. On the banking app, I know there is a security center there. Yeah, I don't know what else, just those two.

Transcript 7

Researcher: Thank you so much. So I'm required to inform you that your participation in the study is completely voluntarily, none of your personal information is going to be shared and you will not be identified personally, so nobody's going to know in the research that this was your responses and also none of your responses are also shared with your line manager. Comfortable to proceed?

Interviewee: OK.

Researcher: So the first question, uh, in terms of the study is, could you briefly describe IT security to me?

Interviewee: Wow. IT Security is basically. Yooh so I have no idea. Background whatsoever. So IT security is basically ensuring that you don't exist. Systems that you are not supposed to access.So if you do access the system and you can prove it's purely for business reasons, then I suppose you can just inform your line manager. But if that was work and you can't prove reasons as to why you access a certain clients profiles, then obviously that is an IT breach or it's a system breach. I think.

Researcher: Second question is what role does IT security policy play in keeping an organization safe from threats?

Interviewee: To make sure that the relevant measures is put in place. Ohh yeah so so. That you don't? They are. They didn't sure that if a staff member clicks on a link that is that the necessary files or the security measures in place to prevent. Cyber criminals from tapping into the banks data.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: I would say yes. you know, most of the time, when there is a breach. It's because of employees not following the processes and procedures.

Researcher: The use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Basically, using simple language. Not everybody's clued up with IT terms, so therefore if they keep the language as simple as possible, everybody would be able to relate to it.

Researcher: OK, if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: Don't mind knowledge is very minimal, so I'm happy with whatever I see at this point in time and the sufficient training that staff has to do on. I don't know. Every so often we get these training and that training that we need to do those questions. You and I, I think it's actually very interesting and sometimes it just brings it home because sometimes you do tend to forget that you need to make sure that before you click on a link, not that we use links that you make sure you hover over the link to make sure that it is secure before you access anything. Yeah. So I think the training that will are provided with is sufficient.

Researcher: OK, in your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: No

Researcher: And lastly, where would you locate our information security policy?

Interviewee: Yeah, it's on the Intranet You putting me on the spot so I know how to get the, but to explain to somebody to go in gate it, that's a different story, but I know it's on the Intranet.

Transcript 8

Researcher: OK, First things first, so I'm required to inform you, Tammy, that your participation in this study is completely voluntary. So you're not under any pressurization

either from myself or from [redacted] or your line manager or anyone else. To participate in the study and your information is is kept securely, so none of the responses that you would provide to the questions today will be shared with your line manager shared with [redacted] or shared with the University of Kwa-Zulu Natal at all, so it's kept completely confidential. You comfortable proceed.

Interviewee: OK. Yes.

Researcher: OK, so the format of the interview is basically questions and answers. They are seven questions. The first question is, could you briefly describe IT security to me?

Interviewee: OK. Alright, so that is security passwords not sharing your password, not uploading your personal information. And the password mustn't be easy. Like your date of birth or something like that.

Researcher: OK. What role does IT security policy play in keeping an organization safe from threats?

Interviewee: OK, so it plays a big role because it protects the company from from the POPI Act or anything like that. It also protects the staff member to make sure that they follow procedure according to the at the Privacy acts.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Yes. Definitely, Sir.

Researcher: OK, the use of jargon and technical terms is commonplace in such policies. How should how should they be improved or simplified?

Interviewee: Because some of the clients don't understand the jargon, we have to then just explain in layman's terms what it means. Otherwise I don't see any issue with the jargons or descriptions that they've used.

Researcher: OK, if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: OK, so we do enough training, so maybe send out notifications like they do to all staff members. Just a refresher or something like that. That's it.

Researcher: OK, in your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Yes.

Researcher: OK. And where would you locate our information security policy?

Interviewee: On [redacted] and the self-service it will be there.

Transcript 9

Researcher: I'm conducting a study around organizational perceptions of our information security policy and its implementation at at [redacted] and part of the research involves a sample

of staff that are surveyed to gain their opinions on some of the aspects that I'm studying as part of the research objectives. So I am required to inform you that your participation in this study is completely voluntary so you are not, you know, pressured or please don't feel pressured to participate in the study. The format of the questionnaire. Basically it's question and answers. They are seven questions which you need to answer and they are open-ended questions. So they are up to you to decide exactly how long or how short the responses need to be. And then the last thing to mention is that your responses are not disclosed to management. So they're not going to adversely affect you. They're not shared with management and they're not shared with the research organization and none of the information or your responses will be used to individually identify you.

Interviewee: OK.

Researcher: Are you comfortable to proceed?

Interviewee: Yeah, that's fine. It's fine Yes. OK.

Researcher: Thank you. So the first question, Tony is, could you briefly describe IT security to me?

Interviewee: OK, I think I did. Security is just basically systems. Systems in place and also probably also kind of a bit of a mental. Umm. Realization of certain aspects of security for computers and computer information and stuff like that would be a T security and and access to systems and particularly stuff that's like. You call it. What you call it? Alright, critical information and and that kind of stuff. What's it? The. Yeah, that kind of stuff. And lock, bank accounts and personal information and and things like that as well. So. So it's just to limit access to the people that need to have access to those systems and to prevent an authorised access to those systems.

Researcher: OK. And what role does IT security policy play in keeping an organization safe from threats?

Interviewee: OK, I think I think IT security policy for that would need to be obviously in place to prevent to prevent. Umm. Data leakage and information leakage to. People know not authorized for that information. For them to do with whatever they wanted to like, for instance, obviously access to very sensitive information like bank accounts and and and and things like that, but also also sensitive information like like like personal details, e-mail addresses, cell phone numbers, ID numbers, identity, that kind of two kind of prevent. Fraud and to prevent. Unsolicited communications and emails and things like that.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Look, I think I think that I, I think there are at equipment like like every like all artist security, I mean as as efficient as the people are putting the security in place equally probably equally efficient others people trying to crack the security as well. So. So it's kind of an ongoing thing you gotta keep trying. Keep ahead of basically trying keep ahead of the bad guys. And the cause I mean, I mean, as clever as the institution and that they get the bad guys also get clever as well. So. So yeah, but I think I think I think our our policy our, our, the the banks IT security policy is is. quite good sometimes for a work situation or sometimes feel that it might be too cumbersome for for ease of work like some systems that I work on for argument sake every five minutes of bloody thing goes off and you gotta log in again and you gotta log in again, you know, gotta log in again. Yeah. So and then certain of the systems it's a login and a 2FA and certain systems is not too far and certain other systems, as I say, go off to five minutes. Certain golf off to half a day so. So so they could be a bit of an

inconsistency there, but also some of the some of them. I mean I don't know why if we've logged into the [redacted] system and we've done our, our our login in the morning and we're on the system, I would I would say that some of the systems maybe don't need to be so tired because you're really in the system. So it's like it's like you go in through the door. oing through the door and through security of a high security complex, we once you in the complex. You can pretty much move around in that complex. OK, smart. Be certain areas that you don't have access to, so there's certain systems that I don't need access to in my work. So then obviously I don't have access to those systems, which is fine. Then basically my security code is not gonna let me open the door to that particular room because I don't have to get into that room. But the rooms that I do have to get into. Umm, sometimes I feel there should be more accessible. As I said, there's one system that I work on literally. I work on the system. If I go off and do something else and come back to that same system 5 minutes later, I've gotta log in again. So sometimes that can be a bit of a pain when it comes to to to trying to work efficiently, because you go back to the system and now you gotta log in again, and then one of the systems I've gotta log in and do two FA every time I log in. So if I go out five minutes for five or 10 minutes and I go back into that same system again, it's a logging again and again.And sometimes I'm I'm not quite sure why does it have to be that secure.

Researcher: OK. The use of jargon and technical terms is common in in in such policies. How should they be improved or simplified?

Interviewee: And look, I think when it comes to when it comes to jargon and some of the jargon is like very hard, sort of hard to say, higher grade jargon yeah, sort of sort of so, so, so, so some of that jargon can be can be sort of like simplified like the real IT boffins have got their own jargon and they going to speak their own language. Uh, uh, but I think I think I I think. You're generally sort of sort of the high grade job and should maybe be be be explained or we put a little bit more layman's terms, but most of the common, let's say the common you use jargon that everybody knows about would kind of be fun to go because everybody knows what what that particular thing is. I can't think of an example now, but but some of the the, the high, the high grade, IT Jargon and the programming terms that they use and things like that as well that that nobody knows about. Umm. The for the people that need to know about it, then obviously it needs to be explained in more layman's terms. But I mean if it's something that that doesn't affect you need. I need to know about it then. What the hell? Why does it need to be explained in layman's terms if it's gonna need to do with you?

Researcher: OK, if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: I don't know. It's difficult to say what improvements need to be made. You can only basically determine what needs to be improved if something goes wrong and there's a breach, then you think, OK, hang on a SEC. Ask. We need to fix that now. But I can't think of hand or anything that needs to be improved. As I said, there are some areas that that maybe this IT security can be dialled back. Sort of a peg or two and doesn't have to be so tight. UM, maybe make the make the initial log into the systems a little bit more secure in that I mean, at the moment when you log into to your system in the morning, when you when you log into the [redacted] system is kind of just your username and password and then you're in. Maybe that initial login in the morning when you're logging onto the [redacted] systems? Should be maybe a 2FA? With that as well. So in your initial login in the morning, when you go into your main screen and you put your F number in your password, there should maybe be a 2FA to get into into that. And then once you're in the door, as I said earlier, once you're in the door, then it should be freedom to move around should be, should be greater than it is on

some of the systems, but it might might be an idea to tighten up initial access initial access onto the system.

Researcher: OK, in your opinion, are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Umm. I don't know. I I wouldn't. I kinda wouldn't really know. Who to contact to to make that kind of a suggestion too? Umm, I don't know what platform there is to use to be able to to to to request something or to suggest something like that as well. But as I said it's it's it's difficult to difficult to maybe determine what needs to be done. To improve the like improve the security unless something unless something goes wrong. But but I've I've been thinking about what I explained to you just now. I'm about the about the tightening up initial access to the systems and maybe relaxing some of the access to some of the systems. Once you're once you're logged in, it's something that I've thought about for a while. I thought. So if you're not so easy to log into the system. But then it's such a pain to actually log into the other systems as well. I mean, like if we take for a given set, I don't know if you know this, if you if if you know the system but could log into oh, God forgive and take requires it too. If I in the morning first thing but then you in Hogan and once you're in Hogan the system is open, it's open. And it only kind of refreshes itself. Maybe sometime in the middle of the day, OK. And the Hogan system is the main customer base is the main customer system. Then the other systems that we have access to this is the Home Affairs, the Home Affairs verification System, information verification system. That system logs off logs of every five minutes and every five minutes you got to log in again with two FA and literally we use that system just to verify clients details on Home Affairs forgiven sake. So when once you're in the [redacted] system, that system should be available for you to, let's say, open up and leave it open on your computer. Because when you log off your computer or when you move away from your computer and you lock you up and you lock your screen, then your screen is locked and. Start. You could even have it two FA on on on your screen unlock again because I mean I mean. How IT systems are in my computer basically goes into lockdown. After five minutes. OK, then the screen automatically locks off the five minutes. So if I'm talking to somebody on the phone as longer than five minutes, must my good Amit from my computer typically such it off? And and then just then, I said. And then and then and then and then and then take it back on again. It's just obviously just a. It's obviously just the password. I'm. But then then the other systems. So say within that it just takes a long time to sometimes relogin, relog in relogin, relog in.

Researcher: OK. Where would you locate our information security policy?

Interviewee: Umm.

I would imagine if you are gonna scratch through, I'll probably find it somewhere on on the, on the what? The [redacted], the my [redacted] page. What's the? Yeah, my [redacted] home page somewhere. I would probably be able to find it on my home page somewhere, but I wouldn't know where to go and look where you gotta tell me. You can't find it now let me take a while for me to go and find it. But I'd probably find it eventually.

Transcript 10

Researcher: So the format of the interview is basically questioned and answers. They are seven questions that I'm going to ask you. Uh, and uh. I'm not going to interrupt you while you're answering the questions. And really it's up to you to decide. You know how long you? How long or how short you want the answers to be? So I'm not going to influence your your

answering in any way. And these questions they are no right and wrong answers. It's just for me to understand your views around information security. Are you comfortable to proceed?

Interviewee: OK. Yes, we can proceed.

Researcher: Perfect. Thank you. So the first question is, could you briefly describe IT security to me?

Interviewee: IT security.

Uh security within the company ITUM information technology. I'm assuming IT censor information technology security system so. Security regarding all our IT hardware software I think I'm sorry I don't know if that was supposed to study for this, but yeah, I think that's what what it would mean.

Researcher: OK. And what role does IT security policy play in keeping an organization safe from that?

Interviewee: I think the role that they play is obviously to ensure that we have the correct systems that will protect us from various threats like phishing possibly and any third party. Threats that might uh be like a risk to the company, so they do play an important role and it's basically to safeguard all our internal systems, I suppose.

Researcher: Do you believe our organizational IT security policies are adequate?

Interviewee: Uh, yes, I think so. I do believe so.

Researcher: OK, they use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Well, we do get training on win, win these training provided I think they do explain the the terms and the jargon in terms of simplification. I don't think you can get more simple than actually explaining what the term is unleash. You check it out yourself, you use a dictionary, but I think it's pretty straightforward.

Researcher: OK, if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: IT security awareness could be improved, maybe more.

More training, but not training where you are responsible to go and do it yourself. Maybe like. Of a form of like a meeting a meeting, things like that. So not what you doing it on your own to to make it more way to everybody. Maybe they could be like. A training session, if I can call it that.

Researcher: OK, in your opinion, are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Um, I'm not too sure I haven't. I don't know. I I don't know.

Researcher: And the last question is, where would you locate our information security policy?

Interviewee: Probably on the Intranet portal.

Transcript 11

Researcher: I'm required to inform you that your participation in the study is completely voluntary. so you will not under any pressure from myself or anyone else, including your line manager to participate in the study and at any point during the interview, if you're not comfortable with the questions, we can stop all you have to say is please stop the interview. And then the second thing that I need to inform you of is that your information will be kept securely. So none of your responses to the questions will be shared with anyone, including your line manager or anyone else inside of [redacted], or will be used to uniquely identify you at the research institution, which is the University of KwaZulu Natal. Uh, are you comfortable to proceed?

Interviewee: Sure, we can proceed.

Researcher: OK, so the the the nature of the interviews. Basically, there are seven questions I need to ask you. I will not interrupt you while you're answering the question and basically it's up to you to decide how long or how short your answers are. But I leave that to you.

Interviewee: OK.

Researcher: OK. Question one, could you briefly describe IT security to me?

Interviewee: OK, sorry, I just need you to elaborate. When you say describe IT security, are you referring to my understanding of it?

Researcher: Yes.

Interviewee: OK, so for me IT security would be. Mitigating risk for like potential fraud, which is cyber related and making sure that the systems that we use are secured in order to protect information of clients as well as internal parties as well.

Researcher: OK, what role does IT security policy playing in keeping an organization safe from threats?

Interviewee: Um, the role that it plays would be to always identify any potential risk that might take place. This is with the connection that you use the system that you use uh, making sure that they are always up to date with today's requirements. In the age that we living in technology wise.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Yes, I do. I think they currently the top notch for me. They currently the first number one. If I can put it that way.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Currently well with the current maybe information that we get, they are currently simplified with the trainings that we have like we do on the Internet. And I think the information that is always synced, it's easy to actually understand everything that is sent out. So yeah.

Researcher: OK, if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: So as I've stated before, Umm, I think Umm, the current uh systems that we are using or our IT is currently number one in my eyes because we are always up to date in

terms of the systems implemented and security that's been implemented the way we verify ourselves in order to access the systems. So yeah, I think they currently there isn't yet more improvement to be done but I think with the. Each as it goes. Umm, there might be some other improvements that that can be done. Yeah. I think more communication because I think with what I've noticed specifically, we normally just get information closer to the time when there's an assessment that is due that we need to, I don't know, maybe this is just me, when there's an assessment that is coming up, but I think frequent communication and awareness regarding IT security issues.

Researcher: OK, in your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: With the assessments, I think that's where we normally do it, but honestly I don't think there is a way per se to say I can log this. Maybe I'm just not aware of it. Where you can log in initiative in terms of ITI think maybe that part.

Researcher: OK. And where would you locate our information security policy?

Interviewee: On the Intranet.

Transcript 12

Researcher: I'm required to inform you that your participation in the study is completely voluntary. None of your information is shared with anyone outside of this call, so it's not shared with your land manager. Anyone at [redacted] or anyone at the research institution, which is UKZN it in and none of the your responses will be used to uniquely identify you. So your information is not shared with anyone and you will not be uniquely identified. Are you comfortable to proceed?

Interviewee: OK. Yes, hi.

Researcher: OK, so the the nature of the interview basically is questions and answers. They are seven questions which I will ask you now and you know it's up to you to answer them.

Interviewee: OK. OK.

Researcher: Oh, thank you. So the first question is, could you briefly describe IT security to me?

Interviewee: Briefly, so IT security for me is measures put in place. You've got your virus software, you you've got systems that would then other than just viruses that would look for spam, SMS and so on. So that's my understanding of IT security.

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: Hmm, I think plays a big role in in the sense that for example I get a lot of emails at times. Today was one of those days where I think at about four or five emails that have gone through where I needed to do e-mail release where it's not to say that everything that comes through is spam, but those ones weren't. But at least that means that with those policies in place, we are able to. Pretty much see if anything is a threat because there's those extra cautions that have been put in place. So I think yes, it does play a big role because without that anything and just about any e-mail can then come through and at times, yes, there are. Times when one would relax if an e-mail has come through and it's gone through

all the measures, but at least with them doing that you know that at least most of the due diligence has been done. We just need to do our part on our side.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Yes, I do. I do. For, for with my experience, there hasn't been any bridge that I know of. So that's what makes me feel that that is more than adequate.

Researcher: OK. The use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Umm, say, uh. So with me. I haven't really come across that much jargon because you would either come across IT related things either through. Policies that are sent out where you're trying that we mostly do things via training. Those trainings are usually put in layman's terms if they are in each organs that are used, they are usually explained in terms of what that particular jargon means. So I haven't really had any issue in terms of that.

Researcher: OK, if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: Umm. If it had to be improved.

Uh, I think probably they are doing that with the training. So I suppose maybe just to. I suppose involving us. I I I suppose in in some in in terms of what is it that we would want to see. Ohh better understanding I suppose on behind the scenes because I suppose we're not IT ticks. So sometimes we would need to understand how these things work, but I I take it it will probably take us from our day jobs at times. But I don't know maybe share insights in terms of look this is where it starts other than just giving US training because training is usually just you know an understanding of what or just giving us info so that we understand what to look out for. So maybe I don't know. That's what I think. But other than that, I think the best way for us to be able to identify what can be changed is having a better understanding of what it takes to get to that and and what are the other angles or avenues that are involved within the IT sector that we might not know of.

Researcher: OK, in your opinion, are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Not that I know of. No, no, I I, I I've never had an opportunity to say we are requested to have input with regards to either IT measures or anything of the sort, no.

Researcher: OK. OK. And where would you locate our information security policy?

Interviewee: I forgot the name. There's something that you interview [redacted] where you would need. Sometimes it would tell you whether there's outstanding policies that you haven't read. You would enter via your employee number. I forgot the name of the actual thing.

Transcript 13

Researcher: I'm required to inform you, Yusuf, that your participation in the study is completely voluntary. You not under any pressure from your line manager or myself to participate in the study and it and it any point during the interview. And if you're not comfortable then you would like the interview to stop. You simply have to indicate so and also I'm required to inform you that your information will not be shared with your line

manager or with anyone out of this conversation, so nothing will be used to personally identify you. Your information is treated securely and your responses to these questions don't go back to anybody at [redacted]. Anybody in line management, anybody in your business unit.

So if you're comfortable, uh, the interview basically takes the format of questions and answers. There are seven questions which you must answer.

Interviewee: OK.

Researcher: OK. You're comfortable to proceed?

Interviewee: Now we can go ahead.

Researcher: OK. Question number one. Could you briefly describe its security to me?

Interviewee: So basically ohh the scheme that it's the type of security that's. Implemented. To control the information surrounding the work that we do with the information that is shared, the systems that we access the. Basically all on anything related to our networks that would be IT security.

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: So basically IT security is important or the role it plays is to secure the bank or to secure any form for that matter, from being breached or any personal or confidential data from being leaked, and also securing basically all information available to us to make sure that we. We are within regulations in terms of security.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: At current from the systems that have worked with and the systems that I have been accessing of recent and since I've been at the bank, yes I do.

Researcher: OK, the use of jargon and technical terms is common in in in in such policies. How should they be improved or simplified?

Interviewee: Umm, I think the use of of language or jargon is now become more common in today's times because we are living in the era of information and the technology technological error so. I think if you are using basically the I mean the language and whatever it may be, they charge and whatever it may be if it ties in with what we are used to then it will assist or will be more beneficial in terms of the knowledge that we receive or share.

Researcher: OK, if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: Umm. I think all round there needs to be more. More training in terms of that so people are more aware of the systems in the procedures and. Maybe even if you know every once a year or every six months, just have like a small like a briefing session, or even if it's like a teams meeting where people join in and we run through the systems and because generally what happens is if you do the training on online or whatever, it may be the training that you do is just a quick one, you trying to get over what it. But if you actually sit in a session, it's sometimes much more beneficial in the long run.

Researcher: OK, in your opinion, are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Uh, currently, I'm not aware of many of the options available, but. Through management and. The networks that you've come across overtime, obviously these can be discussed and brought up and so forth. So those are the only channels currently available at to us.

Researcher: OK. And the last question, where would you locate our information security policy?

Interviewee: On the Intranet.

Transcript 14

Researcher: I am conducting a study within our financial services environment and part of the study requires me to conduct 45 interviews, this being one of them. Around people's perceptions to information security and uh, some of the concepts that I'm trying to understand. Uh, so I am required to inform you that your information is treated securely. And will not be shared with anyone, including your line managers. Not neither will any of your responses. To these questions, and they will also not be shared with anyone who would be able to use them to individually identify you and the nature of the study is confidential. And then this the last thing to mention is that at any point in time, you are free to end the interview. If you are uncomfortable or you would like the interview to end and we will end it there. But the interview does take the format of questions and answers. Are you comfortable to proceed?

Interviewee: Alright, thank you. Yeah. So we can proceed.

Researcher: Perfect. Thank you. So the first question is could you briefly describe IT security to me?

Interviewee: So from my understanding I can describe it as a the kind of security relating to the information technology or now we protect our data when you're using the Internet and also our computers.

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: You make sure that whenever you're connected to the Internet. Whatever you're doing is secret. So we said secreted those kind of things. The information that you are using is secured and then also at protect our clients information. Because that comes from IT security. So there there is no amusing reference to VPN. It comes to a place whereby. You are safe from hackers when using accessing the Internet because. You are restricted to which website you can access using the work them in the laptop of organization. So you can't just access any website? So VPN helps a lot.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Yes, I do believe that. Because when using the system, you can't just go to any website, only the website which are sacred you cannot access.

Researcher: OK, the use of jargon and technical terms is common in such policies like IT security policies. How should they be improved or simplified?

Interviewee: So I think that with today's world? I think that that. People are more familiar with them, so it's not that really difficult for people to understand those terms when it comes.

So I see. So for me, I don't think they can be simplified even more better because in these days everyone is familiar with the IT always and stuff, so it's easy to understand them.

Researcher: OK, if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: So I think it will help with. When I was challenging the cybersecurity as well, if it can be improved so that everyone they can see that whatever we're trying to do, we're not trying to steal their information or whatsoever, but we're trying to protect that information. So because sometimes I'm client, when you're doing this kind of maybe as you are trying to verify them through the system, you ask them some question. They're not conceivable asking them, I think. If they can be those kind of awareness program to let them know whenever you ask such question or just trying to make sure that your data is protected so most people they don't feel comfortable being. As lot of questions which they never thought you'd be able to. Obtain them. Those days off IT because we are able to extract that of a certain person and then when asking them those questions, all patient questions, they feel intimidated and then they don't feel comfortable. Because at some point I remember I this other side, I was doing my secret check with them. Using that DSO, I was asking them the question that the system was able to obtain and they were they were not comfortable proceeding. They thought maybe I'm just trying to still die information. So I think our next program should be. Implemented.

Researcher: OK, in your opinion, are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Yes. So I'll, I'll be answering this based on what I I deal with in a daily basis when it comes to meet the challenges that I I have expressed in the past is when I'm doing security check. I was thinking of it is a culture with people. I think the time. Or maybe diminish that is given to us to to approve, or maybe to do those security checks are challenging because sometimes we're dealing with old people. They're not really familiar with the technology. So the time frame that is given to us to use is limited. So some of them, they fail to, they tend to fail. Living, though, is the rightful owners of the account.

Researcher: OK. And lastly, where would you locate our information security policy?

Interviewee: From the [redacted]. That's where you can look at it.

Transcript 15

Researcher: I am required to inform you that your participation in the study is Completely voluntary. You're not under any pressure for myself, your line manager, or anyone else in [redacted] participate and secondly, I need to inform you that your responses to the questions today will be treated anonymously, so none of the information that you provide to me today will be shared with your line manager, with anyone at [redacted] or will be used to individually identify you in the study. So before we proceed, I need to ask you consent, are you comfortable to go ahead?

Interviewee: Yes.

Researcher: The first question is could you briefly describe its security to me?

Interviewee: IT security, uh. As for me, it's. The information that we receive regarding the security and the videos that we watch.

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: It makes the employees away because we always so busy, so. I like. Money laundering and those things that we get to watch, it helps a lot.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Yes. Umm. The things that they send us to do every time it does help so. I can say it's adequate.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Ohh. Maybe put it more in like layman's terms, maybe in brackets it should make it easier for us.

Researcher: OK, if IT security awareness so specifically awareness could be improved, what would that entail in your opinion?

Interviewee: Umm, I don't for me. It's fine for me.

Researcher: OK, in your opinion, are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Can you say that again?

Researcher: So in your opinion, do you believe that there are adequate opportunities available to you to shape our IT security program or for your own input to be incorporated?

Interviewee: Umm, like I said, the videos that we watch help a lot. And it is interesting.

Researcher: OK. And the last question, where would you locate our information security policy?

Interviewee: Ohh. On the [redacted] website.

Transcript 16

Researcher: So thank you so much for availing yourself this afternoon. So firstly I'm required to inform you that your participation in the study is completely voluntary and none of your information is going to be shared with anyone or used to individually identify you. And additionally, none of your information or your responses are shared with your line manager. So are you comfortable to proceed?

Interviewee: OK. I'm fine. Thank you.

Researcher: Cool. Thank you. So question one is, could you briefly describe IT security to me?

Interviewee: OK, I see. OK. I think within our business, the ideas. Securities actually very good, because if you think now for sometimes it can be very irritating that you need to approve, you can't work without a phone anymore. Because you need to approve everything. So. If someone steal your phone, they can't do it, so that part I think that is good. So I don't have a problem. I think it is up to standard.

Researcher: OK.

Interviewee: Lots of improvement over the years happened.

Researcher: OK. Can you tell me what role does IT security policy, specifically the policy play in keeping an organization safe from threats?

Interviewee: It's important so that we can keep up to date with all the scams and things that's happening nowadays. So I think that we need to get up regular updates or information.

Researcher: And do you believe our organizational IT security policies are adequate?

Interviewee: Yeah, I do believe it.

Researcher: OK. And the use of jargon and technical terms is common in such policies, how should they be improved or simplified?

Interviewee: More, maybe more simple language so that we understand and not like complicate the jargon that they use.

Researcher: OK, if IT security awareness specifically, so I'm specifically talking to awareness now then, IT security could be improved. What would that entail in your opinion?

Interviewee: Umm. Well, I think at the moment we getting like regular. Training and not training more. But you call this thing that they ask us to do. Not training, but this and sign not assignments. Assessments. So I think we get. Get enough of those.

Researcher: OK. In your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Can you repeat that question please?

Researcher: So in your opinion, do you believe that they are adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Umm. No. I never seen anything we our input was asked.

Researcher: OK. Where would you locate our information security policy?

Interviewee: Umm. On the [redacted] page. Do you know I don't know the specific even page.

Transcript 17

Researcher: I'm I'm required to inform you, Nicole, that your participation in the study is completely voluntary. So you are not under any pressure either from myself, your line manager or anyone at [redacted]. Uh to participate in the study. In addition, I'm also required to inform you that none of your information will be shared with anyone. So any response that you provide here on this call is not shared with your line manager, not shared with anyone outside of [redacted] and will not be used to individually identify you. The format of the interview is 7 questions which are required to answer. They are open-ended questions, so it's really up to you to decide how long or how short your responses need to be. Are you comfortable to proceed?

Interviewee: OK. Sure.

Researcher: Cool. Thank you. So the first question, is, could you briefly describe IT security to me?

Interviewee: Basically. The countless measures that, if in be takes in order to secure. Anything IT related? Virus firewalls I mean antivirus. Passwords, system identifications, you name it.

Researcher: OK. And can you tell me what role does IT security policy play in keeping and organization safe from threats?

Interviewee: I'd say having tools available to identify threads, making employees aware of how to identify threats themselves. I'm having the relevant reporting departments in place to assist with. Suspected or confirmed threats and then also processes in place on how to. Deal with those threats if anything's been breached or or not breached, that kind of thing.

Researcher: OK. And do you believe our organizational IT security policies are adequate?

Interviewee: Adequate at driving me insane, yes. But yeah, no, I think if [redacted] does a pretty good job with with the IT security in general.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Umm. I don't think I'd be able to give a a good answer on on on that one because my dad is a IT boffin. So I learned a lot from him, so a lot of the jargon and I know, but. Sometimes you know in the policies and stuff, if there is a specific word that obviously most people aren't gonna know. Maybe just have like a blustery attached to the the policy, or even just in brackets. Just the breakdown of what it. terms in layman's terms.

Researcher: OK, if IT security awareness so specifically awareness could be improved, what would that entail in your opinion?

Interviewee: Umm. Thing is, they they do a lot of communication with regards to the awareness. I mean it's emails, it's. Those pop up notifications. It's training on self-service. The thing is just that I don't think that all employees actually. Absorb it. I don't wanna say negligence, but you know, sometimes those kinds of things slip your mind especially. Depending on your background and what department you in, how old you are, how take save you, all that kind of thing?

Researcher: OK. And in your opinion are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: We I don't know about any way that I can give my input to be honest. But I mean, I I don't feel that my opinion would matter anyway because I'm not an expert in the field.

Researcher: OK. And can you tell me the last question, where would you locate our information security policy?

Interviewee: [redacted] If I remember correctly.

Transcript 18

Researcher: I need to inform you that your participation is Completely Voluntary. So none of what you say here is, you know, conveyed to your align manager is not shared with anyone

inside of [redacted] or outside the bank. And none of the information is. You know it's it's going to be used to personally identify you and then the other thing to mention is that your participation in the study is completely voluntary. So you're not under any pressure, any duress, to participate. Are you comfortable to proceed?

Interviewee: Yes, I am.

Researcher: The first question question number one, could you briefly describe IT security to me?

Interviewee: So it's basically our privacy and all those things.

Researcher: OK, what role does IT security policy play in keeping in an organization safe from threats?

Interviewee: I think it's as to do with uh, it avoids a certain security violations such as fraud and all those things.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Yes, I do.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Umm. Well, I don't know if it can be improved because I I know the jargon is quite we don't understand most of it. So my my be the wording use it in more layman's terms.

Researcher: OK, if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: For me, It would be like if you've got an IT problem like the turn around times could be improved.

Researcher: OK. In your opinion, are there adequate opportunities available to you to shape our IT security program all for your input to be incorporated?

Interviewee: What can I say with this one? Actually, we don't have much time to get so much involved in it and to do what it but it would be nice if we get involved somehow if it is in connection with regards to our work.

Researcher: OK. And then lastly, where would you locate our information security policy?

Interviewee: On the server, on the. Home page.

Transcript 19

Researcher: I need to first let you know that your participation in this study is completely voluntary. You're not under any pressure, any duress, from myself, from line managers or anyone at [redacted] to participate. And secondly, to mention to you that your information is how securely so none of the information the responses that you provide to me today will be shared with anyone or shared with line managers and used to. You know, used to personally identify you. Are you comfortable to proceed?

Interviewee: I am comfortable.

Researcher: OK. So question number one, could you briefly describe IT security to me?

Interviewee: IT security?

Researcher: Security, yeah.

Interviewee: No, to be honest, I'm not quite sure what's IT security.

Researcher: OK. Could you tell me what role does IT security policy play in keeping and organization safe from threats?

Interviewee: I would. I would be thinking that. It by ensuring that all. Uh, systems secure for the protection of the organization. IT security would ensure that no hackers are able to get through to the systems of the organization or the business that would be their main. I think their their main objective.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: I mean it it they seem to be adequate enough at this point because what I would say is. The system seemed to be doing what they need to do in a sense that they always protect the interest of the organization. The data of the organization and the information that's captured of clients. So I would think that the, the the policies are sufficient enough in in support of that objective.

Researcher: OK. The use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: They should be simplified in a way that when it's even a, you know, a a teenager or a child can understand them how they are explained. They can be explained in a way that's in layman's term like. Without any complicated jargon.

Researcher: OK, if IT security awareness specifically, so I'm specifically talking about awareness could be improved. What would that entail in your opinion?

Interviewee: To improve it, I would say the best people who can assist in improving it would definitely be hackers, because you do find organizations that are dedicated into testing systems. You know other systems from other organization to ensure that there's no loop holes or threads. So in, in, in terms of improving it, I would say definitely it would be involve like a A company that's dedicated towards operating as a hacker and to to to test run systems. The systems that organization has or [redacted] has in order to ensure that there's no loopholes that other hackers can exploit.

Researcher: OK. And in your opinion, are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Yes, there is. There is those opportunities. Uh, I know there's the other one on. I forgot what it's called when you have like all these innovative ideas, you can always post them on one of the websites on the organization and these opportunities they do take them into considerations. It's not that you when you after posting something you don't get feedback. So I would say in terms of. You put the painting and the programs. They do facilitate employees to and and value their their input.

Researcher: OK. And the last question. Where would you locate our information security policy?

Interviewee: The [redacted] website.

Transcript 20

Researcher: So I am required to inform you that your participation in the study is completely voluntary. You're not under any pressure by myself, by your line manager or anyone in the organization to participate. It's completely voluntary. And then secondly, I need to inform you that none of the information you provide here is shared with anyone. Your information is kept confidential, so none of the answers that you provide are shared with anyone, and they also not shared with line managers. Also, your answers will not be used to individually identify you. Are you comfortable to proceed?

Interviewee: Yes, we can proceed.

Researcher: Cool question number one, could you briefly describe IT security to me?

Interviewee: IT security. OK, let me try to understand the question IT security. OK, I see it's a. It's a department that deals with the. Technical or the system of the organization. So I think IT security will be. The the security that the IT department is offering in order to save guide the information of the company or the system of the company.

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: To make sure that, uh. The the. The cyber criminals don't have an access to our clients information or to gain an access to to the organization information

Researcher: Do you believe our IT, our organizational IT security policies are adequate.

Interviewee: Yes, I do believe that.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: OK, firstly, by knowing the audience. To to to know the audience. And then once you know the audience, your audience, then you will be able to. To know who will understand the. The the the terms and then if not then to our clients. I think it should be just a simple English.

Researcher: OK. OK, if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: OK. Everyone will will be. Everyone will understand the papers of. IT security and then. And then the importance of. Protecting the clients information. And the information of the business.

Researcher: OK, in your opinion, are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: How can I put this? OK IT security should. At least Umm. I just to the technology, the more the technology changes, there should be more innovations on our on our IT security to. To to to be updated with the changes on the technology.

Researcher: OK. Last question, where would you locate our information security policy?

Interviewee: Ohh I'm not 100% sure with that question.

Transcript 21

Researcher: I'm required to inform you that your participation in the study is completely voluntary. You're not under any pressure by aligned manager, myself or anyone at [redacted] in terms of your participation, it's completely voluntary. And then the second thing I'll let you know, I need to inform you around is confidentiality. So the information that you provide your responses will not be shared with anyone at [redacted], your line manager or will be used to uniquely identify you. Are you comfortable to proceed with this interview?

Interviewee: Yes, you can proceed.

Researcher: Question number one. Could you briefly describe IT security to me?

Interviewee: Umm, I would say that it's the type of security whereby a measures or yeah measures are put in place in terms of protecting the business and. Information critical information. So for example, like sending out an e-mail to. Someone who's not part of the business, sometimes they would block such emails to avoid confidential information to be shared with other people.

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: Can you repeat that again?

Researcher: What role does IT security policy play in keeping an organization safe from threats?

Interviewee: Ummm security measures whereby. I'm for example with cards to the the the the the platform that I work at. We need to to have all of our platform secured either through your passwords that in each individual must set up for themselves. Umm, the other thing, the world that they play to to make sure that the information is protected is by having for example your. Umm antivirus platform software so that the information is protected at all. Talk all times and nothing that is malicious may impact the business.

Researcher: OK. And then do you believe our organizational IT security policies are adequate?

Interviewee: Yes, I firmly believe so. Like I stated, I've tried to. To even send things to my personal emails. But those emails won't go out due to those securities.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: And repeat the question again, sorry.

Researcher: The use of jargon or acronyms technical terms is common in such policies. How should they be improved or simplified?

Interviewee: I think just two to to avoid confusion. Umm, the must just either. Have a. I'd say a. Information whereby a supporting information, wherever those terms are been explained. Let's say if we taking all you signing up for either software or something, they should be some. guide, which explains all information, which explains those Jack on all. They can just use a language where which anyone, even if it's a layman, will understand the language.

Researcher: OK, if I IT security awareness specifically could be improved. What would that entail in your opinion?

Interviewee: I'd say that maybe. Having. Awareness of the meetings or something maybe once in a month. Whereby. We are reminded of. I'm things that we should be careful of, things that we should have avoid to do. With regards to the platform that we use is which information to share and which information not to share.

Researcher: OK, in your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Umm yeah, I'll say theres adequate opportunities available to to me.

Researcher: OK. And then lastly, where would you locate our information security policy?

Interviewee: We find them in one of our one of our platforms that we use, which is the first thing [redacted] share point whereby we find every information that we need to know either with regards to the products or.

Transcript 22

Researcher: Your participation is completely voluntary. You're not under any pressure from your line manager or anyone in[redacted] , including myself, to participate, so 100% up to you if you want to participate or not. And then secondly, to inform you that your responses. I'll treat it confidentially and none of the information that you provide here will be shared with your line manager or anyone else at [redacted], or used to uniquely identify you. Are you comfortable to proceed?

Interviewee: Yes, we can proceed.

Researcher: OK. Question one, could you briefly describe IT security to me?

Interviewee: OK, I think IT security is. Uh, IT people who are responsible for protecting us on our information or the information of clients are both online and offline.

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: Uh, I think it guides it, guides the IT people and also us on how to. On how we can protect the information our information online.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Ah, I'm not that familiar with the with the policies, I think I would still need to to get some more information in order for me to answer that question.

Researcher: OK, the use of jargon abbreviations and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Uh, I think you you need to use the language that is, uh. Normal the language of everyday people, not the language of IT, specialist. So that the uh, the general public can understand.

Researcher: OK, if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: I think they shouldn't be just one module or like a one full module at one time. I think it should be like an everyday thing or an A regular basis thing that we are reminded of the policies and how these things work.

Researcher: OK, in your opinion, are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Yes, I think this interview is an example of that.

Researcher: OK. And then lastly, where would you locate our information security policy?

Interviewee: Yeah. Yeah. No, I'm not that familiar with it, but I think on the [redacted]

Transcript 23

Researcher: Your participation in the study this afternoon is completely voluntary, so none of the information that you provide to me will be shared with your line managers. Anyone in [redacted] or used to individually identify you and your participation is is 100% voluntary. So if you don't want to participate, that's perfectly fine. You can just tell me and we will end the call. But if you would like to participate, are you comfortable to proceed?

Interviewee: Yeah, we can proceed.

Researcher: Question number one. Could you briefly describe IT security to me?

Interviewee: OK, so I just security is basically all about ensuring the security for. You know, for our laptops to ensure that you know that the the data that is that we access to the laptops is protected and also it doesn't get shared by anyone like for instance with regard to the laptop is just make sure that things like locking while you leave your laptop it's it's common practice and also not sharing passwords or your username and stuff. And also regularly changing you know. They log in details and. Yeah, that's how I would describe it.

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: OK. So it's it's it's it's a form of awareness like within an organization. So that we can also have good practice to and ensuring that you know what, no, you know no access from outside or any threads to our data that we deal with because we didn't with customer data and you know if anyone gets hurt of that then it's it's gonna be it's gonna be a bigger problem because. You know, it means that people will be able to access, you know, the money. So any information that they can use, you know, just to to, to tarnish or destroy the the customers that we you know we deal with.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Yes, I do believe that they are because you know those policies, you know it's something that we all need to abide by and also, you know, understand what's being stipulated in the. So I I think they are adequate in you know people are keeping you know their practice or ensuring that you know what everything is secure.

Researcher: The use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: I think if we can have maybe a glossary maybe for those jargons so that we you know I think that is a better way of simplifying them. For instance if someone you know doesn't understand a certain dragon who can you always reference back to that glossary.

Researcher: OK, if I IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: I think I like this kind of, you know, like the emails you there are security and there are emails that are sent with regard to security. I think maybe also having like this kind of you know interaction with someone from you know risk it's I think it's gonna you know put strength into the awareness process. Yeah, that's, you know, go like regular communication around that and also encouraging, you know, people to continue practicing that aspect of security. I think, you know, we, you know, that will improve it more.

Researcher: OK. And in your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: So I think I'm maybe I must just be. You know, I have, I haven't really look at the policy but. Like I do practice certain security. You know, things that I know of that we need to, you know, apply while working in an in a banking environment. So I think also. In terms of inputs and I think yeah, as as you know, as someone who work with the data as an employee, like if I have certain input on the police, I think that should be incorporated so that you know we can all practice the same thing like if I pick up something that is you know you know will be a thread and I try to raise it, maybe there's need to be a platform where that I don't know if there's a platform that's already existing where we can always put you know share our inputs with regard to the security around it. But also you know to give an input someone is to you know, be aware of how you, how they currently policy looks and also the practices around it.

Researcher: OK. And then lastly, where would you locate our information security policy?

Interviewee: OK, it's it's on. On our intranet.

Transcript 24

Researcher: Participation in the study is 100% voluntary, so you're not under any pressure by myself or anyone that [redacted] including your line Manager 2 participate firstly. And then secondly, I need to inform you that your responses to my questions this afternoon are treated confidentially and they will not be shared with your line manager or anyone at [redacted], and neither will they be used to individually identify you as part of this study. Are you comfortable to proceed?

Interviewee: OK. OK. Yes, I'm comfortable.

Researcher: Uh, question number one, could you briefly describe IT security to me?

Interviewee: OK, I think it's regarding to protect mostly information. All of our clients as well as protecting devices that we currently use in order to execute our daily duties. Yes, that's what I can think of.

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats? So here's specifically I'm asking about security policy and and its impact on keeping an organization safe.

Interviewee: OK, its actually difficult for me, but I think they have to be controls that are put in place for us to follow. Let me think of an example. Like for example when you attend training, they do mention to you that you're not able to download any software which is actually has to be done by the IT or approval themselves. So I think the security mostly comes from the IT itself guiding us what to do as per as per policies also that we normally have to agree on on what you call that. Umm. On my IQ, something so it's actually in general the IT people will provide us with guidance on what to do and what not to do. That's all I know from my side.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: For me, yes, I do think so. I do think with the introductions of like for example VP VPN's for me. I think the adequate is just depending on the employee themselves in order to follow the instructions, but I personally believe it's adequate to protect our security. Yes, that's my answer.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Yes, that's why I need the problem too. That one is a problem because I think as an IT specialist. When you communicate with me in a. Knowledge that I don't understand. Definitely what's the point of communicating that information to me in the 1st place because I will never understand. So I think they need to. Be aware that not all of us are actually expect in terms of IT, so they should use the knowledge that everyone can understand and avoiding the use of acronyms of which we totally don't even know what that means compared to a person who's actively involved in the IT environment. So the jargon is a problem for my side.

Researcher: OK, if I IT security awareness specifically could be improved. So I'm specifically wanting to know about awareness, security awareness, if it could be improved, what would that entail in your opinion?

Interviewee: Uh, so far. Had can't say much on that one. Because I think with a little knowledge that I have in terms of ITI just accept what I've been told. Because I do believe it is the best. Decision that has been made from IT perspective, so I can't say whether it's. Not up to standard or not, so I can't really comment much on that.

Researcher: In your opinion, are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Umm, no. No. I don't think you know there's no such.

Researcher: The last question is where would you locate our information security policy?

Interviewee: It's on [redacted].

Transcript 25

Researcher: I need to inform you that your participation in the study is completely voluntary, so you're not under any pressure from your line manager, myself or anyone at [redacted] to participate. It's completely voluntary. And the second thing I need to inform you is that your responses provided to me here today are treated securely and confidentially, so

nothing that you provide to me here today is going to be shared with line manager or would be used to uniquely identify you as part of the study. Are you comfortable to proceed?

Interviewee: Yes, definitely.

Researcher: OK. So question number one, could you briefly describe IT security to me?

Interviewee: Right. So if that would be talking about information that comes through? That needs to be referred to to IT. Really it's a more sharing of information or getting into links that mean be insecure. So all that kind of information or phishing and all then would need to be referred to to IT. We can refer to to group ID T if you know how to, but our own in-house IT would be able to intervene and and take care of such matters that are suspicious.

Researcher: OK. Question number two, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: Yeah, that is. I mean that is very, very important to protect us as employees from being exposed to fishing, for instance, might also a helps protect a clients information as well. Because I mean now we are looking at to we are legally bound to keep the clients information secure. And obviously there's some metals like poppy. We need to be cognizant of that so that we don't overshare information or even share information with them. The people that are not organizations that are not intended to actually get access to the information. So IT comes in. It's more like a defensive have mechanism for us really to protect everyone, clients, the organization and generally all the stake holders release. So that and obviously they actually come in as well in the form of recommended training for employees so that we can protect the clients information and obviously clients give us their information on the basis and belief that. We will keep it safe, so IT comes in there to highlight to us. How we can actually go about protecting the information and obviously making themselves available to? To help us as a reference point so that we can really keep this information stuff.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Yeah, I believe they are, but obviously we we need to to, to, to, to, to keep abreast with the trends in the, in the market. We really need to be agile. We need to be flexible. We need to be open to new information, carry out our research. As long as we don't stand still and keep abreast with the changes that are happening currently and expected changes in the future, then we should be adequate. But as long as really we we keep abreast with the trends, then we should be OK. It's never enough. That one thing that I take cognizant of is never really enough because criminals are always a step or two ahead of us. So yeah, I I think you we are well equipped to deal with it with the threats, but obviously we need to to keep evolving as well not to be left behind.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: You know, we talk things like you abbreviations and abbreviation may mean one thing to an IT individual and may mean another to me as a client service consultant. So it would actually help for them for the IT. People to our technicians, to, I mean to simplify them. If there is a jargon that is, they feel it's more IT related than they need to clarify it, simplify it, maybe bracket it so that everybody is reading from the same pair edge. Yeah. Really not to assume anything. I think that's very, very important that you do not assume that the next person is going to interpret it. The Jaco and the way you do even it's gravity as well. It's very, very important for us to illustrate to the stakeholders how we have the the

jargon is how important it is to interpret it the way it's intended to be interpreted. So. That is very, very important. Whoever is communicating should take cognizant of the fact that not everyone understands things the way they do. As the technical people. So it's very important to take into account that.

Researcher: OK, if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: UM, really? I think from my side I benefited a lot from the trainings, online trainings, online tasks that we have to undertake the assessments. And obviously the IT I think is the one thing that needs to be done. Also the visibility of the technical people we used to have, for example chamanga and when he left, it was almost like the IT team became almost distant to me. They are not visible. I know we don't always come into the office, but I still feel that it will be very, very important for us to know our IT team. For them to be visible really to interact with us and almost like really rubber stamp the importance of in I mean information security in the business. But the assessments that we do online, maybe we could do with more possibly. They need to be rolled out more frequently and obviously the importance of those assessments also needs to be drummed up with employees because we do not have to be reminded of the importance of going on to [redacted] and doing those assessments. Everyone needs to take responsibility. Ownership of those so that we don't burden our managers with reminding us to do them.

Researcher: OK. Question #6, in your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: I want to believe that the opportunities are there. It's up to individuals to actually take them up. I mentioned that the IT team is not visible, but it may be up to me. Really. It's up to me to get up and find them. So yeah, I want to believe the opportunities are there, but it's up to the individuals to avail themselves to be able to acquaint themselves with the the security information, procedures and projects.

Researcher: And then the last question, where would you locate our information security policy?

Interviewee: Umm, [redacted] is actually a good place to to have that information.

Transcript 26

Researcher: I'm required to inform you that your participation in the study is 100% voluntary, so you're not under any pressure by your line manager. Anyone at [redacted], including myself, to participate. So at any point of this interview, if you would like to to opt out, or if you would like not to participate, please let me know. And then secondly, I need to inform you that your information will be treated securely, so none of the information that you provide to me will be used against you, it will not be shared with your land manager, anyone at [redacted] and it will also not be used to individually identify you as part of the study. Are you comfortable to proceed?

Interviewee: OK. Alright. Yes.

Researcher: So question number one, could you briefly describe IT security to me?

Interviewee: So according to my understanding IT security is about securing who has access on our environment in terms of our the servers that we use and also who has access

on our applications. So to protect ourselves we use firewall rules within our environment to we don't like provide access to everyone else but rather to certain people. All sudden business units. And also in terms of uh, access, we don't provide access to everyone in the business except to the people who needs those kind of access into the applications

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: They have to make sure that they apply a patching and. Their software protection against viruses. And also I think infrastructure plays a huge role in terms of taking care of the security walls within our organization.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Yes. I do believe that.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: I think it it it can be simplified in terms of that everyone within the organization would be able to to read those kind of jargon words that I used within our our organization and they are able to understand what it means. So I think simplicity is important to to help. Everyone was in the organization, even the people who are outside that security IT security role.

Researcher: OK, if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: OK, I think the the compliance training that the organization provides to. To to its employees, then that is one of the tools that helps us to understand what IT security means and how to protect ourselves from anything that is attracted to to the organization in terms of a security.

Researcher: OK, in your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Uh.

As it as it stands.

Uh, maybe it's because I don't know where to find those kind of opportunities, but I haven't been exposed to any of those opportunities where I can have input in terms of security.

Researcher: OK. And then lastly, where would you locate our information security policy?

Interviewee: On the Intranet.

Transcript 27

Researcher: OK, so I need to 1st inform you that your participation in this study is voluntary. You're not under any pressure to participate. So at any at any point, you can decide that you don't want to participate. And it's entirely up to you. And then the second thing I need to inform you of is that none of the information that you share with me would be shared with your line managers. Or anyone at [redacted] or used to individually identify you. UM, so your information is kept secure and confidential. Are you comfortable to proceed?

Interviewee: Yes, but how was I selected? Because the I know there was a link which is Umm, if you're on a participate onto this direct click. Yes on that. I don't remember. No. So you have been randomly selected to participate in this in the interview.

Researcher: So, so, uh, basically I've used a random selection of employees across the group, and you happen to be one of the fortunate people to be included in my sample. Yes. OK, question number one, could you briefly describe its security to me?

Interviewee It's basically, uh, just having policies in place to secure our organization and Umm data that our organization has.

Researcher: What roles does IT security policy play in keeping an organization safe from threats? So here specifically the emphasis is on security policy. OK.

Interviewee: But basically, just uh, it facilitates data incredulity. Uh, sorry, integrity and confidentiality.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: I'm not sure.

Researcher:: OK, why do you say not sure?

Interviewee: Yeah, OK. I mean IT, right, well there's a lot of things that are questionable you know. UM, when it comes to users versus business and stuff. So it may be adequate, but I think there's just lack of awareness.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: There should be some sort of a a thesaurus with each and every jargon you know, like a contract. You get a contract. It states that that uh person is the individual who contract is the document, like something like that. Something that would explain those joggers, you know, for a person who maybe who's new into the information space or IT space so that they get to know the the the key time, the terms that I used, you know, because it can get confusing for someone who's like fairly new in a specific field.

Researcher: OK, if I IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: Refresher training causes hey, because sometimes we we do this causes and then over like after a year, we like forgotten all like this. There's something new that's that's that's that's happening that we're not informed or we're not made our way of in a form of a security training course like we normally have so it shouldn't take a year I think it should be like every three months they should be like a refresher course edging onto the new stuff that you know hackers might you know try and in in in.

Researcher: OK, in your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: I would say I'm not sure because I've never had an opportunity where I was, you know. We says today where I was asked of an opinion in terms of UM, information security, you know, safeguarding for could put it that way.

Researcher: OK. And finally, where would you locate our information security policy?

Interviewee: [redacted] Intranet.

Transcript 28

Researcher: I'm required to inform you that your participation in the study is voluntary, so you're not under any pressure by your line manager, myself or anyone at [redacted] to participate. And then secondly, I need to inform you that your responses will be treated confidentially, so none of the information you provide to me at any answers will be shared with your line manager, anyone at [redacted] or used to uniquely identify you as part of the study. Are you comfortable to proceed? Are you ready to go ahead?

Interviewee: Yes.

Researcher: Question number one, could you briefly describe IT security to me?

Interviewee: Um, I think IT security is. The people responsible for. Securing or protecting the information that we use within our space. Uh, the people who are always checking for those? Um, maybe risks, you know? And putting on measures to mitigate such things. I think that's what it is.

Researcher: Okay, what role does IT security policy play in keeping an organisation safe from threats? So here specifically I'm asking around security policy.

Interviewee: While they play a big role, because this is Cline's information that we're dealing with and with all the fraud that is happening on a daily basis, we we need all the IT needs to make sure that the information is protected. Not only the clients information but everyone's information as a whole. Because it's not only the client that is targeted, it can be an employee who can be targeted. So it is very crucial for it to make sure that they have all the measures in place to protect. Each and every person, as well as their information so that they don't, um, fall into fraudulent activities or find themselves being involved in such things. So I think they play a major role on a daily basis.

Researcher: OK, do you believe our organisational IT security policies are adequate?

Interviewee: Yes, I do.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: I think we need to use simple, simple terms, right? Because sometimes I get to to log a query and I'm like what in the Lord Jesus are they talking about here? You know, so, um, our terms in our space and the IT terms are not the same. I will need somebody to to explain to me what exactly are you Fed into you know, if you're working with something, you are used to it, you know what it means, but the other person wouldn't understand. And it's not because they are slow or they are stupid or anything, but it's because they are not used to these terms on a daily basis. They are not exposed to them. So if we can simplify the wedding, that will help as well.

Researcher: OK. If IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: Right. Having those, um, I don't know whether it's it's not daily communications that we get but if we can always get those communications that okay, this is what is happening, please be aware of this. I think we do get those patient emails now and again, but if it can be on a regular basis so that we are kept on the loop we are kept away and if the team can also detect those spam emails. Before they get through to us, you know, try to to handle those emails before they get through to our boxes. You know, we work with

boxes where we get a lot of emails. So if maybe they can have a system to detect such emails before they come through just to to make sure that we work effectively as well instead of having to send an e-mail to the team to say please release this for me please. You know, I think that can help.

Researcher: In your opinion, are they adequate opportunities available to you to shape our IT security programme or for your input to be incorporated?

Interviewee: This is not done. Even at the current moment. We still have issues that have not been resolved, you know, and I make a promise to the client to say I'm gonna send you your statements. Then I tried to download the statement. I'm not able to. What do I go back and say to the client?

Researcher: And then the last question, can you go where would you locate our information security policy?

Interviewee: Um, I think on the intranet.

Transcript 29

Researcher: Hi, I must Inform you that your participation in this study is voluntary, so you're not under any pressure from your line manager, myself or anyone at [redacted] to participate. This is a completely voluntary participation, and then secondly, I need to inform you that your information is treated securely, so none of the responses that you provide here this afternoon will be shared with anyone at [redacted] or used to individually identify you as part of the study. Are you comfortable to proceed?

Interviewee: OK. Yes, I am.

Researcher: OK. Question number one. Could you briefly describe IT security to me?

Interviewee: OK, so IT security to me means the protection of information and measures put in put in place to protect the companies information, specifically the clients information. So they that's basically measures that are put in place.

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats? I'm specifically asking around the policies. What role does IT security policies play in keeping an organization safe from threats?

Interviewee: OK, so the policies, the policies guide us in how we should.

How everything should go and what we should follow, what we need to do and what we need to avoid because you know, as humans we make miss mistakes, but then having policies will help us to be able to protect the company's information and to also stay protected ourselves.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Ohh well I can't say much but I think that they are. Yeah.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: OK, so there needs to be maybe sessions like we they can explain what sometimes mean because sometimes using jargon can be explained, can be very confusing.

for like normal people, don't work in the IT department, so we need maybe like classes, uh, and so forth. They will educate more in explain thoroughly what everything means.

Researcher: OK, if I IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: Yeah, basically having more awareness like maybe classes, sessions just to remind us, because sometimes you do forget that, OK, this is what we have to do to protect ourselves and so forth. So maybe having certain reminders to and trust awareness classes would really help.

Researcher: OK, in your opinion, are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Uh, uh. I don't even know. I don't think so because I'm not sure if ever we can give our input regarding that. So I don't think so.

Researcher: OK. And then lastly, where would you locate our information security policy?

Interviewee: I think they were on the [redacted] or I am not sure.

Transcript 30

Researcher: I'm required to inform you, that your participation in this study is completely voluntary. You're not under any pressure. Any duress from myself. Your line manager or anyone at the [redacted] to participate. And then secondly, I need to inform you that your information and the sponsors that you provide here this afternoon are treated confidentially. None of the information that you share with me would be used by align manager or to individually identify you as part of the study. Are you comfortable to proceed?

Interviewee: OK. Yes.

Researcher: OK. Are you comfortable to proceed?

Interviewee: OK, let's proceed it.

Researcher: OK. Question number one. Could you briefly describe IT security to me?

Interviewee: My understanding is the protection of the information. It can either be at a workplace or information in general. Lesson my personal information. Sorry, that can be IT security you like. We're talking about things like passwords that we put as a form of security.

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: Umm, it plays the role of. It plays a role of keeping it safe from things such as scammers. Yes, things such as scammers and. Yeah. Any any form of? Any form of yeah, any form of scammers that can endanger the the organization as a whole. Especially when it comes to information like clients information as well as the employees information as a whole.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Definitely.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Maybe. OK, maybe they can try to use a languages that is more clear to anyone. Anyone that says someone like me, who who doesn't deal with IT, so maybe they can simplify those languages that they use as a IT specialist.

Researcher: OK. If IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: If it could be improved, I think let's say for example, if ever we can, let's say in, in, in the organization that we are at as [redacted], we can at least have class classes where we can train next people like general employees like me who doesn't know anything about IT. Maybe train them like explain to them how few things works around IT I think. We can definitely look into that.

Researcher: OK, in your opinion, are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Yes, there is. There is.

Researcher: OK. And lastly, where would you locate our information security policies?

Interviewee: We can look at it on on the self-service link.

Transcript 31

Researcher: 'm required to inform you that your participation in this study is voluntary, so you're not under any pressure to participate. You have not been asked to do so by your line manager and you are not. Pressurized to do so, and then the second thing to inform you is that your responses are treated confidentially and none of the information that you provide will be shared with your line manager or anyone at [redacted] or used to. Uniquely identify you. Are you comfortable to proceed?

Interviewee: Yes, I am.

Researcher: Question number one, could you briefly describe IT security to me?

Interviewee: Protect the information.

Researcher: OK, what role does IT security play in keeping an organization safe from threats?

Interviewee: You have to. You have to. To lock your system. You have to everything you're doing that you have a password so that no one can login into your.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Yes, I do.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: I think OK, according to my understanding everything like I have to to note that abbreviation by heart. I need to write it down so that I can like no it better.

Researcher: OK, if IT security awareness, so I'm asking specifically around awareness. If just security awareness could be improved, what would that entail in your opinion?

Interviewee: They're login details.

Researcher: OK. In your opinion, are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Yes there are.

Researcher: OK. And then lastly, where would you locate our information security policy?

Interviewee: Email and online banking.

Transcript 32

Researcher: OK, so I I'm required to inform you that your participation in this study is completely voluntary. So you're not under any pressure from your line manager and you wanted [redacted] or myself to participate firstly. And then secondly, I'm required to also inform you that your information is treated securely and confidentially. None of the responses that you provide to me today will be shared with your line manager with anyone at [redacted] or will be used to individually identify you as part of the study. Are you comfortable to proceed?

Interviewee: Yes

Researcher: OK. Question number one. Could you briefly describe IT security to me?

Interviewee: It's more like. Umm, not allowing us to install anything that would like to to install on our system. It's more like managing what it's going out of the system. What is coming into the system like for example, last year when I was with Jakki wanted to to upload the protect video but it didn't allow me because of the firewalls that we there, which I believe is entire living we we will not allowed.

To maybe upload things on our system or so that is the whole purpose for IT security just to store our information to to to restrict what is going in on, on, on the system and going out of the system. Something like that.

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: Yeah. You're maybe looking unwanted. Information to go into the system. Yeah, like we charging your phone, like, uploading stuff on your system is I believe that's the that's their responsibility to. To see that our system doesn't get the what do you call it? The viruses and that's their duty that you don't get hacked, that you information is safe. You know that nobody can go into the system and. Go into your accounts. Yeah.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Yes thus far I I believe so. I. I feel safe logging into my Internet, banking on my work laptop, then using my own laptop at home.

Researcher: The use of jargon and technical terms is common in such IT policies, right? How should they be improved or simplified?

Interviewee: That's not an easy one. Just to put it in plain simple language, but it's just that the jargon it's it's it's it's it's a jargon. I believe that's there's no other way that you can make it easier for us since we not working in the IT space. So we always have to ask what do they mean by this? There is a better way I believe that you can make it easy but not. Almost everything. Some, some is just those things that comes out with the. With it. Because it's technical, so I believe even the the jargon on the language is also technical. I don't know if there's something that can be done there? But if there is maybe to reduce it to a simple language for us who are not working in the IT space to. Be able to really don't understand, but yeah.

Researcher: OK, if IT security awareness, so I'm specifically talking about security awareness could be improved. What would that entail in your opinion?

Interviewee: Like, yeah. Umm. Umm. I can't think of anything now. Because I believe whatever that is put they it's the the the test that we normally write on [redacted] . These sufficient enough for us because that is. That much that we know. So we don't know the loopholes that are there, but what is provided to what is given to us on the table that is. What we know, that's where we could that it limits us today, doesn't push us to. Want more to say? We believe that, you know, when something is not genius, but place you don't normally feel that there's a need for you to look fair, that you feel that what is given to you, it's efficient and the day. Whatever it is that we do have for us, they are sufficient. We don't know if there's anymore, anything more that we need or you guys need to be aware of.

Researcher: OK, in your opinion, are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Ohm. Yeah, I believe through our process is that's the way we normally. Pick up the loopholes, but then. Yeah, I believe there's always something because you know, the technologies is evolving. So there should be somewhere where does the loophole where guys maybe are not aware of the other trends that the other businesses are doing. So we can always get information from our external clients, our children out, they they so technical. So yeah, it's just, uh, takes maybe somebody. But I think we just need somebody internally who can just. Interview I would lines extend. I didn't see what processes. What is it that they do to secure? I was systems for the better. So. Yeah. If somebody can be somebody or the team that deals with that strictly to do that, I'm more like a research of some sort I can be interested in that because currently I'm doing project management. I haven't even checked in which space one to be on project management. It can be part of the project. I believe it can be one of the projects to do that, maybe to see. We can things be incorporated for the betterment of the security processes and the likes.

Researcher: OK. And then the last question, where would you locate our information security policy?

Interviewee: So I'm not sure. I'm not sure.

Transcript 33

Researcher: So I need to inform you firstly that your participation in this study is completely voluntary. So you're not under any pressure. By myself, your line manager, or anyone at [redacted] to participate. And then secondly, I need to inform you also. Uh, that your responses are treated confidentially, so nothing that you say to me here would be shared with

your line manager or would be used. To individually or uniquely identify you, are you comfortable to proceed?

Interviewee: Yes, I am.

Researcher: OK. Question number one. Could you briefly describe IT security to me?

Interviewee: It is security is basically protection on your valuable information that's held on your your electronic equipment.

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: It plays a big role.

Researcher: OK. You you wanna elaborate on on, on that at all?

Interviewee: Because if there's no security, then your information could be accessed easily and manipulated anyhow. And you could be at risk of identity theft or. Other things. As well.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Yes, they definitely are.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Umm, I'm not sure. I'm not sure.

Researcher: OK. If IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: Oh then. No, it definitely would be good, a good thing. To let more people know about the safety. Their safety.

Researcher: OK. In your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: For me, at the moment I'm I'm not sure I'm not. A big IT person, so I'm I can't really say there.

Researcher: The last question, where would you locate our information security policy?

Interviewee: The main system, the portal. [redacted].

Transcript 34

Researcher: So thank you so much. So firstly I need to inform you, Alistair, that your participation in the study is completely voluntary. None of your responses are going to be shared with line managers with anyone at [redacted]. Secondly, none of the information that you provide to me today will be shared with anyone and also not used to. Basically, to individually identify you and that's your participation in the study is completely voluntary. So are you comfortable to proceed?

Interviewee: Oh yes, indeed.

Researcher: And yeah, if you're ready to to get going, question number one, could you briefly describe IT security to me?

Interviewee: No problem. Thank you. IT security is basically. An IT department that assists us with basically putting up firewalls, preventing all threats that could possibly attack the bank system or even us as employees. So they basically help us put in the measurements to prevent any fraud from taking place or from us divulging information that's not supposed to be divulged to public.

Researcher: OK. Question number two, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: Uh. The policy basically is in place for my understanding to assist all banking stuff to understand what measurements IT can put in place to make sure that they safeguard us from either going against banking regulation because the bank is also regulated by regulatory boards to make sure that. Basically, information isn't how could I say, recklessly divulged to the public or shared with non banking stuff.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Uh, yes, I do cause due to currently we have. What I've seen in places the two FA. SO 2FA basically links it to your employee number, so we never. I'm gonna access the systems. I need to log in with my employee number and before allowing me to log on to the system, I need to verify that via 2FA, which makes it quite secure and it also actually indirectly informs me if it with a message I had to come through to my phone and knowing I haven't accessed my systems that there could be possible fraud in the background. So here's I feel it is adequate in that form.

Researcher: OK and the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: I think in that case we need to bring it to layman's terms and.

Stop referencing them because I believe jargon is then derived off of the actual main word itself. Which to public knowledge, people wouldn't know what the system was named or anything like that. We could rather call it what like. If in be, uh, secure verification. For people to more or less understand, and it's not to be linked to, like let's say for example, two FA is mostly known in IT. As to what the detailed breakdown of two FA is, but generally in the bank I'm almost stuff. Still a little wonder what the wording to have a stands for.

Researcher: OK, if I IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: The awareness of it. OK, I think general notifications that would pop up on systems like, for example systems that I would frequently access just to create an awareness of what measures are put in place to safeguard us on those systems just for frequent reminders. Also like, you know, that general pop up, remember to refresh or restart your computer now and then based on it's just to educate the end user. And make him aware that, like let's say for example updates need to run overnight. That gentle info that would be OK, because that would also remind me to also do certain things more consistently. Unlike it being a now and then. Thing that we do on our side as end users.

Researcher: OK, in your opinion, are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Ohh. No, I don't think so. So I haven't had a actual. Sit down with any IT group to find out as to how I feel about. The interaction with the systems itself. There was some systems, I feel that IT should be rather sitting in with us as frontline users. To have more a front or end user experience and also pick up on. What if there is really restrictions that we do receive what restrictions we have and just for us to also understand as to the limitations of the system and what we're allowed to do and what not? Itself. So yeah, I think they should be more of a a quite a collaboration conversation. Around that.

Researcher: OK. And the last question, Allister, where would you locate our information security policy?

Interviewee: 1st place I would go and look under is. Uh, what's this? Myself service is at my service. I figure it's under my the my[redacted]. Let me tell you, I'll tell you the system now, we apologize. OK, so from my point of view I'd said search it on the 1st Rand Group SharePoint.

Transcript 35

Researcher: I'm required to inform you that your participation in this study is completely voluntary. So you're not under any duress, any, any pressure from your line manager or anyone at [redacted] to participate. It's completely voluntary. And then the second thing to let you know is that your information or your responses to the questions in this study, will be treated confidentially. None of your responses will be shared with line managers or anyone at [redacted] or used to individually identify you. Are you comfortable to proceed?

Interviewee: OK. I'm sure so everything is totally anonymous.

Researcher: Yes, that's correct. So none of none of your responses will be directly tied back to you.

Interviewee: OK, 100%.

Researcher: So the first question, could you briefly describe IT security to me?

Interviewee: In what format? If we talking about it as a whole, we're talking about IT security in in what we do as what I do.

Researcher: Your general understanding of IT security.

Interviewee: For me it is security is, uh, having a secure platform in what I do, how secure the platform is security in terms of the platform. If it's if I'm authenticating the platform enough to to bring security for the client. If my system is giving that form of security. That's that's my that's. That's what I look at it from that level. So if if the question is based on that, that's what I'm answering IT security, the validity of it. If if you asking me whether our system is secure enough, I'm going to say if you're working out in a percentage. And I I'd say 70 to 80%, it's not secure enough.

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: It plays a very important role.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Umm. And I'm going to say yes and no.

Researcher: OK. Yes, you're going to elaborate on the yes and elaborate on the no?

Interviewee: Umm, OK, so I'm gonna say I'm going to say yes and no. I think sometimes our governance it's not. I looked at properly. There's certain things that we know we are we've got our IT policies are are are OK. And then they certain things. Well, IT policies are not. And I was security in line of our systems speaks to the business process that's number one and the number 2 then our system is. And there's a bit of a collapse. So that's why I say yes or no and we've got secure chat and then you can sit on a weekend and you can make a payment and then it can Sit with a link where that payment is now sitting because of secure chat, you'll all have you're all [redacted] app is messed up because of secure chat. I've never worked on a system where your banking is hit with the secure chat, so that's why I'm saying yes or no.

Researcher: The use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: It's too it's very high level. We need to come down a level. We need to speak to the consensus of feedback. We need to come to a level where everyone understands the jargon and the term is really high explained. We need to always come down to a level where everybody, including your end user, understands the level. Not everybody is IT. Related there'll be people that will be segregated into. Or don't understand IT and then you've got people that understands IT. So we need to to be. Related to everyone. I think your jargon needs to speak to everyone, not a segregated selection of of people.

Researcher: OK, if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: Number one, look at your governance policy #2 make sure that your end user is happy with with your start to your end results #3 make sure that testing is always done correctly #4 make sure that your system is always aligned to your business process and #5. Make sure that whatever implement whatever sign off. That you've done your final sign off from your higher level management. Umm. In terms of security, make sure it's it's within line of the governance, that it's not going to interrupt. Your business because sometimes like I'm saying, it's gonna pick up something that's going to affect security. You're gonna have something that's gonna break the system. And you know, it's gonna be something small that's gonna pick up that's going to. That's going to have someone go in and withdraw 2,000,000 who is not your client.

Researcher: In your opinion, are there adequate opportunities available to you to shape our it's security program or for your input to be incorporated.

Interviewee: Umm for me I don't know. OK, I'll say yes and. Well, I'm developing my own self in order to do that so. I don't know. I'm. I'm I'm. I'm on the fence there. So I don't know. Yes and no. So I'm developing my own self on that. So I'm gonna be on the fence on that one.

Researcher: And then the last question, Lorraine, where would you locate our information security policy?

Interviewee: On the intranet.

Transcript 36

Researcher: Before we begin, we begin. I need to inform you, Michelle, that your participation in the study is completely voluntary. So you're not under duress by anyone at [redacted] and including your line managers to participate. And secondly, to inform you that your information is kept securely and confidential, none of the responses that you provide to me here today would be shared with anyone or used to individually identify you or shared with your line manager. Are you comfortable to proceed?

Interviewee: OK. Yes, I am comfortable to proceed.

Researcher: Let's begin. Question number one, could you briefly describe IT security to me?

Interviewee: OK, so basically measurements put in place by obviously the IT team and to ensure that our systems are secure. Firstly because I if I should think that company information is not Privy to everyone. So that would be maybe installations or softwares put in place or uploaded onto the OR assets of that. Of the of the. The company, and so like your network, I would like for example we have to use VPN which is a secure measure to add to to use the the the the the company systems out of the out of like the office let's say like when you're working for at home or you working at a restaurant or let's say you just working remotely so like VPN would be one of them. And I think in one of the assessments that was mentioned that you rather use like your Wi-Fi that's provided by the company and not public Wi-Fi because of the information that's on the laptop, it's only Privy to you and not the public. So I think that's my understanding.

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats? So here I'm specifically wanting to find out about the policy security policy.

Interviewee: Ah. So obviously it it plays a vital role cause I'm a can't imagine what what would be the business, what would be of the business if there was no like. Like secured system is also secured networks loaded for us so. So that would be like example. I used the game was your VPN, but it's it can't we can't. We cannot function without it and obviously that was built in by the by by the IT team to ensure that it's dates available. And so I don't know.

Researcher: The third one, do you believe our organizational IT security policies are adequate?

Interviewee: OK. Yeah. Yes, I'm firmly believe that it's equate. It's amazing what let's say if there is an incident to be investigated and it requires IT's intervention and it's amazing what data the IT team can pull, pull up. To be honest. I've been amazed, to be honest. So I think it's very efficient in our space.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Yeah. So in my, in my experience, I've had the frustration way a lot of IT jargon was used, and it was not certified and because of that we then had to get into a teams call so that they they they explain it better. So I think to avoid wasting time by getting into the teams called that's information can be simply fly. It's simplified on the calls that we log. Instantly cause sometimes when they respond to your call using their IT Jag and they under the assumption that you you know what it is. It's like even in presentation sometimes and the IT jargon that you sometimes you don't really understand. So if that can be simplified

because I'm thinking even when I deal with my clients I can't use the the the terms that we would use internally with the client because the client doesn't know these terms so. If that can be simplified, it would make our jobs easy and it would save time.

Researcher: OK. And if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: I I think one thing I would like to see is getting the audience to engage more and then like maybe have questionnaires in between you know and then you can offer maybe even a chocolate just to reward the person with the correct answers. Like just to keep people engaged in the conversations, not just be a plan presentation from beginning to end. If we could have like. And it's just to see if people are actually catching paying attention to what's being presented and keeping them on the spot. If we can have something like that, I think it would help. Because other than that, if you just if as a presenter you just speaking, just presenting, presenting and not asking questions like engaging with the crowd, then at some point people start losing their focus or attention. So if we can have something like that.

Researcher: OK, in your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: I wouldn't say yes, and the reason why is because I wouldn't even know who to go to if I wanted to share my ideas. So if the opportunity is there, I should. I think it should be more advertised, or we should know about it more than we would definitely use that opportunity to share our ideas.

Researcher: OK. And lastly, where would you locate our information security policy?

Interviewee: I don't know, is it on [redacted] .

Transcript 37

Researcher: I need to inform you firstly that you are not under any pressure, any duress, to participate in the study. It's completely voluntary. So you know your align managers have not asked me to ask you. This has got nothing to do with line management. It's got nothing to do with sort of your day-to-day duties and you are free to stop participating at this in the study at any time. If that is your wish. And then secondly, it's to inform you that your responses to any of the questions today will not be shared with line managers. It also won't be used to individually identify you in terms of the study or to, you know, create any problems for you in your day-to-day duties. So if you're comfortable to proceed, can you give me a go ahead?

Interviewee: Yes you can. Please go ahead.

Researcher: OK. Question number one. Could you briefly describe IT security to me?

Interviewee:OK, I think it's something like that is being used to prevent maybe unauthorized users from getting inside a network, something like that.

Researcher: OK. Can you tell me what role does IT security policy play in keeping an organization safe from threats? So yeah, I'm specifically asking around the policy IT security policy.

Interviewee: OK, so it prevents scammers and also it prevents us from being scammed.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: I would say it is adequate because it's helping us a lot. From people who are scamming us or hackers things like that.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Umm. It can be improved by our notifying us or sending us emails to specify the things that they do.

Researcher: OK. And if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: I'm not quite sure about that, but. It can help employees to. Understand proper cyber hygiene or security risk.

Researcher: OK, in your opinion, are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Umm. Not really, because I'm not specifically sure about this program yet, so I don't think I have any opinions regarding this.

Researcher: OK. And lastly, where would you locate our information security policy?

Interviewee: I think via the internet.

Transcript 38

Researcher: So I'm required to inform you that your participation in the study is completely voluntary. You're not under any pressure. You're not under any duress either by myself, by your line manager or anyone at [redacted] to participate. And secondly, your information is treated completely. A confidentially so none of your information will be shared. None of your responses will be shared with your line manager. With anyone or used to personally identify you, are you comfortable to proceed?

Interviewee: Yes, I am.

Researcher: So the first question question number one, could you briefly describe IT security to me?

Interviewee: Security is all about keeping being able to keep your information safe. But setting your information safely.

Researcher: Okay, what does IT security policy play in keeping an organization safe from threats?

Interviewee: Umm by creating password, always updating their systems. Making sure that it is secured. Yes, system is secured.

Researcher: OK. And do you believe our organizational IT security policies are adequate?

Interviewee: Yes.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: I think by using simple term that we are we are used to that we were using every day.

Researcher: OK. If IT security awareness specifically, so I'm specifically talking about awareness could be improved. What would that entail in your opinion?

Interviewee: Maybe by doing those training face to face with each and everyone of us, I don't know.

Researcher: OK. And in your opinion, are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: No.

Researcher: OK. And where would you locate our information security policy?

Interviewee: I am lost, I don't know.

Transcript 39

Researcher: So I'm required to inform you that your participation in the study is completely voluntary. None of the information that you provide to me will be shared with your line manager or used to individually identify you, and that's your participation is not under indigenous by your line manager, myself or anyone at [redacted]. So if you would like to not participate in the study, you're welcome to do so, but your information will be treated securely and none of your information shared. Are you comfortable to be to proceed?

Interviewee: Yes, I am comfortable to proceed.

Researcher: Question number one, could you briefly describe IT security to me?

Interviewee: OK, I'm from my understanding IT security is. Digital security in terms of. How can I put this in terms of like your cell phone, your computer, you know, electronic devices?

Researcher: OK, what role does IT security policy play in keeping an organization safe from that? So I'm specifically asking around IT security policy, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: OK, Umm it helps by keeping. The employees. I don't know how to answer that, but it helps by keeping employees. OK, OK. OK. It helps by keeping employees. Keeping the sensitive information about the the company or. All this other staff members safe, it secures information for the company.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: Yes, they are, I believe so.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: OK by by using a simple simple English for everyone to understand.

Researcher: OK, if IT security awareness specifically could be improved. So the question here is specifically around security awareness.

Interviewee: I think it'll entail offering colleagues and employees more training about the IT compliance or IT security info. I think that that's the main reason.

Researcher: Question #6, in your opinion, are there adequate opportunities available to you to shape our IT security program or for your opinion and your input to be incorporated?

Interviewee: Yes. Yes, they there are, there are. There there is. Yes, I believe so. There is adequate information for me to to be able to assist.

Researcher: OK. And then lastly, where would you locate our information security policy?

Interviewee: The [redacted] Website

Transcript 40

Researcher: I'm required to inform you this morning that your participation in this study is completely voluntary. So you're not under any pressure by your line manager or anyone at [redacted] for your participation. So thank you for volunteering and in the second thing to inform you is that none of the information that you provide here in one of your responses will be shared with line managers or used to, you know, individually identify you in the study or be shared with anyone. So the responses that you provide here will be kept confidential. Are you comfortable to proceed?

Interviewee: All right, no worries.

Researcher: Thank you. Question number one. Could you briefly describe IT security to me?

Interviewee: Alright, according to my understanding IT security on our side regarding the communication of how we use it, I believe it is the way. We used the communication as a internal people in terms of using the systems of like business and sharing information that we are not supposed to be sharing with external parties and so forth. And we go through through certain trainings for sharing information and so forth and also passwords on my end. I believe that is what IT security is all about.

Researcher: OK. Thank you. What role does IT security policy play in keeping an organization safe from threats?

Interviewee: OK, they play a role in terms of the restriction many and accessible sites are, for example social sites and at the and appropriate sites which. The business doesn't want to be, for example, find itself being hacked by external parties or accessing in our internal data and so forth. So I believe that it takes place that role the. Hence they have to train our participants on a regular basis regarding how IT should be carried out.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: They are very close, they just keep us more alerted and be cautious about accessing certain things that we should be on the lookout as always personally and also business weather related to the business.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Ohh, by so far uh. They use of jargon. I've not paid much attention to that one but but then. The on terms of use of jargon, I clearly don't know how that one. Uh is carried out in terms of IT.

Researcher: If IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: All and since ohh everything is always updating and moving towards. So. Uh software from hardware. So uh, mostly. Uh, most of the things won't be comfortable with us moving to them. And by that. So we just need to adapt to it and the changes that it comes with and security and awareness it brings amongst us.

Researcher: OK, in your opinion, are there adequate opportunities available to you to shape our IT security program all for your input to be incorporated?

Interviewee: Alright, after so far they're up to standard and I'm very I'm impressed with them to that instance.

Researcher: OK. And lastly, where would you locate our information security policy

Interviewee: [redacted]

Transcript 41

Researcher: I am required to inform you that your participation in the study this afternoon is 100% voluntary. So you're not under any pressure by a land manager, myself or anyone at [redacted] to participate. And then secondly, I need to inform you that your information will be treated securely and confidentially. So none of the responses that you provide to me today will be shared with your line manager with anyone at [redacted] or used to uniquely or individually identify you. Are you comfortable to proceed?

Interviewee: OK. Yes, OK.

Researcher: Question number one. Could you briefly describe IT security to me?

Interviewee: OK so. My understanding. IT security will be. The level in which system secure. In the company. We clients information companies information is protected from Hercules. That that, that will be my understanding of it.

Researcher: OK, what role does IT security policy play in keeping an organization safe from threats?

Interviewee: Strengthen or secure Then the company or businesses. I think it will. It will mess up the the the business reputation. The that their systems won't be breached by hackers. Is importance of by changing to be strong so that they can then take the client experience information and the business. Uh formation so that everything kept intact.

Researcher: OK. Do you believe our organizational IT security policies are adequate?

Interviewee: In my belief, I I think it is. I have never heard any scandals.

Researcher: OK, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: I would say it has to be simplified for employees who are not in the IT department so that they couldn't also. I think they can also, yes, they can also understand

how systems so. Can be simplified for other employees are not in the IT field to to understand also.

Researcher: OK, if I IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: Please repeat that statement once more.

Researcher: If IT security awareness so specifically awareness could be improved, what would that entail in your opinion?

Interviewee: Yes. Yes, I I think it will. It will help benefit the the the company a big deal because it will the the awareness will it it, it will be an awareness of for all employees in [redacted] to know. That. That the IT security is a very important part of everything. So they can also be aware and also help. In stopping any glitches or hacking scandals, anything to protect the business.

Researcher: OK, in your opinion are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: So I'll I'll say yes, because we do receive training. I think it's an annual basis, if if I'm not mistaken, in which we we do. And we we do receive emails that you need to do your training. But I do think awareness is there from from the the risk department to umm, I teach us and make us away. Those because we do receive those trainings.

Researcher: Do you believe that there's opportunities for your input around awareness around security, around training? Do you believe that there's opportunities? You know, for your input to be taken into account or incorporated ?

Interviewee: Yes, yes, yes. If if maybe on those trainings you can. And have. Like a I think it like a checkbox or something to to write we we all employees can write what they think can be can be needed to to add on those. So I I do come yes I do I do. Can I say? Agree. Yes, I do agree with with with input from employees so that it makes them because they they they can be something, some, some something one of the employees can see that maybe happened to them where they can then provide feedback to to to our IT team then so that they can maybe improve the processes their side.

Researcher: OK. Where would you locate our information security policy?

Interviewee: [redacted]

Transcript 42

Researcher: Effectively what I'm doing a little is I'm conducting a study to the university. Of course, Zulu Natal and sanctioned by by[redacted]. To understand how information security policies are implemented. Within the bank, part of this process requires me to conduct interviews to gain some insights from staff, and I I need to conduct 45 of these interviews and you are randomly selected to participate. You are one of the interviewees. So the first thing I need to inform you is that your participation in the study is voluntary. So if you don't want to participate, you must let me know if you're not comfortable and in the second thing to inform you is that your your responses, so any of the information that you provide to me today in response to the questions will not be shared with your line manager or anyone at [redacted] in order to uniquely identify you. So nothing that you say here will be attributed to you directly in the study. I'm the only one that knows your responses. OK. Are you comfortable to proceed?

Interviewee: Yes, I am comfortable to proceed.

Researcher: OK. Thank you. So question #1.Could you briefly describe IT security to me?

Interviewee: OK, IT security is basically my understanding what IT security is that it tries to prevent any unauthorized personnel from accessing the systems that we use on a daily basis. So hence we have your unique F number and your own password that you set for yourself to try and minimize any unauthorized personnel to have access to the systems that we use and. Yeah, to try and protect the bank and its clients information.

Researcher: OK. Thank you. Question #2, what role does IT security policy play in keeping and organization safe from that. So here the emphasis or is on security policy?

Interviewee: So basically IT. Uh security policy protects the organization in that. There are systems that are in place. That I used to identify. That used to identify and authorized access. And then it protects the companies, computers and networks. I hope I'm correct. Is there correct answer? Incorrect answer?

Researcher: No, no, there is no correct or incorrect answer. Remember, these are questions and I'm trying to understand your views.

Interviewee: Ohk OK.

Researcher: Question #3 do you believe our organizational IT security policies are adequate?

Interviewee: Yes, I believe our organization, IT security policies are adequate in there. They are all updated every once in a while.

Researcher: OK, question #4, the use of jargon. And technical terms is common in such policies. How should they be improved or simplified?

Interviewee: Umm. Jargon can be improved by giving definitions to the ones that at least understand it and know it is not common in most cases because some people are not familiar with the IT jargon that is used. Yeah, that's it.

Researcher: OK, question #5, if IT security awareness specifically could be improved, what would that entail in your opinion? So if if if there was something in in terms of awareness. IT security awareness that can be improved. What would that look like in your opinion?

Interviewee: Maybe having workshops once in a while? And I can't say they should not have charts at the office because people really come to the office. Yeah, I haven't workshops in once in a while and sending advertisements of emails informing us that would work.

Researcher: OK. #6, in your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: No, they are not. Or if they are, I don't know of any of them. I'm not aware of those opportunities.

Researcher: OK. And then the last question, where would you locate our information security policy?

Interviewee: On [redacted] and [redacted] .

Transcript 43

Researcher: Hello and thanks for your time this afternoon. I must Inform you that your participation in this study is voluntary, so you're not under any pressure from your line manager, myself or anyone at [redacted] to participate. This is a completely voluntary participation, and then secondly, I need to inform you that your information is treated confidentially, so none of the responses that you provide here this afternoon will be shared with anyone at [redacted] directly or used to individually identify you as part of the study. Are you comfortable to proceed?

Interviewee: Yes

Researcher: Thanks. Could you briefly describe IT security to me?

Interviewee: Security is like cybersecurity that strategy and prevent the unauthorized access to organizational assets like including computer network and data.

Researcher: OK, question #2. What role does IT security policy play in keeping an organization safe from threats? So specifically I'm I'm I'm asking about policy, what role does IT security policy play in keeping and organization safe from threats?

Interviewee: Pardon. I'm not sure these things.

Researcher: Umm question #3. Do you believe our organizational IT security policies are adequate?

Interviewee: Yes.

Researcher: OK, question #4, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: There should be a training material. Uh for all users?

Researcher: OK. Thank you. Question #5. If IT security awareness specifically could be improved, what would that entail in your opinion? So here I'm specifically talking about awareness initiatives for IT security. If they could be improved, what would that look like in your opinion?

Interviewee: I will prepare knowledge presentation like that. I'll be prepared knowledge presentation. OK, I'll prepare knowledge, presentation or course like that.

Researcher: Thank you. And then question #6 in your opinion. Are there adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Yes.

Researcher: OK. And then the last one, where would you locate our information security policy? So if I asked you to look to, to, to, to send me the policy, where would you find it?

Interviewee: Its on banking website.

Transcript 44

Researcher: Hello and good afternoon. There are a few disclaimers or Ts and Cs to mention first. So your participation in the study is voluntary. You've been randomly selected.

You can opt out of the study, so if you don't want to proceed, we can stop the interview here. But I would appreciate it if you, if you did proceed. And then secondly, none of the information that you provide to me in this afternoon will be used to uniquely identify you. So none of your responses will be tied to you directly as part of the study. So there's not going to be your name published in the study with your answers or anything like that. So in terms of your consent, are you comfortable to go ahead?

Interviewee: Alright, so I'll hope hope I'll be a suitable candidate for you. Alright.

Researcher: OK, so question #1, could you please briefly describe IT security to me?

Interviewee: Oh, I see. Security. OK, so I think in my own ways IT security has to do with the product protection and the safeguarding of the the group or the [redacted] resources. Information resources, yeah.

Researcher: OK, question #2, what role does IT security policy? So I'm specifically asking around policy. What role does IT security policy play in keeping an organization safe from threats?

Interviewee: So. I think I think it, it shows that uh. Like all the employees. And the stakeholders like they follow. Like a way to ensure that the privacy is is protected of the clients and the resources that are[redacted], that belongs to the [redacted] are protected and they're well saved guarded.

Researcher: OK. Thank you. Question #3, do you believe our organizational IT security policies are adequate?

Interviewee: Yeah. And I think, yeah, I think they are adequate.

Researcher: OK. Question #4. The use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: I think the the most used solution is to actually start by. OK, having those keywords just to explain the terms and the jargon that is used. On the document before someone actually go through them or someone like if while you're busy reading, you can just go through that indexes just to see what other terms and jargons mean, actually mean.

Researcher: OK, question #5, if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: How can I put this? IT security. Like has been, will be like improved in such a way that we now it is like would be more assured that our our our our information it is well protected right and it it actually minimizes the risk of. Like they say about attacks and. Like hacking. The server attacks and. But the the vulnerable, like the vulnerabilities that we are susceptible to now, they they will be protected, yeah.

Researcher: OK. Question #6, in your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Yeah. I don't know.

Researcher: OK. And then the last question, where would you locate our information security policy?

Researcher: I think it's available on the Internet.

Transcript 45

Researcher: Thank you so much for your time this afternoon. I'm conducting a study at the University of KwaZulu Natal around information security policies and their implementation in organizations, the target organization is [redacted], so this study is approved by [redacted] Information security and your participation in this study is voluntary. So none of the information that you provide to me or that you disclose is shared with anyone internally or line managers. It is also not will not be used to uniquely identify you. So none of the responses will be used to. To single you out, are you comfortable to proceed?

Interviewee: Yeah, I know, that's fine. Okay, comfortable.

Researcher: Could you briefly describe IT security to me?

Interviewee: OK, so IT security. Is the setup that stops people being able to get into our systems that are not supposed to be in them, and it's stops us giving information to people to help with this.

Researcher: OK, question #2, what role does IT security policy? So I'm here. I'm specifically about specifically asking about security policy. What role does IT security policy play in keeping an organization safe from threats?

Interviewee: So the policy puts together the right people that have the knowledge of. The stuff that needs to be protected and then obviously puts the best people in place to then train the staff members on what to do and how to handle different situations.

Researcher: OK. Question #3, do you believe our organizational IT security policies are adequate?

Interviewee: Yes.

Researcher: OK, question #4, the use of jargon and technical terms is common in such policies. How should they be improved or simplified?

Interviewee: So the jargon. This gets a bit difficult, but the jargon, um. The jargon and it needs to be identified and then explained on the side. It's obviously that's not obvious to anyone, but it's it's difficult to say what's obvious for some and not obvious for others though. So yeah, no. From my side it would be even the stuff that obviously that looks like something that the the layman wouldn't know then should just be you know the defined or explained.

Researcher: OK. Question #5 if IT security awareness specifically could be improved, what would that entail in your opinion?

Interviewee: So obviously I mean obviously we we have no knowledge of of things that are going on for the groups specifically. So like the pop-ups when they were launching their. What was it called? You know, when you requested new PC and all that kind of stuff or that kind of thing, those kind of pop ups with IT related things were all security related things would be useful.

Researcher: OK. Question #6, in your opinion, are they adequate opportunities available to you to shape our IT security program or for your input to be incorporated?

Interviewee: Currently for so many employees who do what I do, no.

Researcher: OK. And then the last question, where would you locate our information security policy?

Interviewee: So I would say the the Intranet or you know the [redacted]

Appendix 10: Ethical Clearance

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

22 September 2020

Mr Riyadh Sayed Razack (200202020)
School Of Man Info Tech &Gov
Westville Campus

Dear Mr Razack,

Protocol reference number: HSSREC/00001838/2020
Project title: Case Study: Evaluation of the comprehensibility of information security policies in a South African bank.
Degree: Masters

Approval Notification – Expedited Application

This letter serves to notify you that your application received on 19 August 2020 in connection with the above, was reviewed by the Humanities and Social Sciences Research Ethics Committee (HSSREC) and the protocol has been granted **FULL APPROVAL**

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment/modification prior to its implementation. In case you have further queries, please quote the above reference number. PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

This approval is valid until 22 September 2021.
To ensure uninterrupted approval of this study beyond the approval expiry date, a progress report must be submitted to the Research Office on the appropriate form 2 - 3 months before the expiry date. A close-out report to be submitted when study is finished.

All research conducted during the COVID-19 period must adhere to the national and UKZN guidelines.

HSSREC is registered with the South African National Research Ethics Council (REC-040414-040).

Yours sincerely,

[redacted]

Professor Dipane Hlalele (Chair)

/dd

Humanities & Social Sciences Research Ethics Committee
UKZN Research Ethics Office Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Tel: +27 31 260 8350 / 4557 / 3587
Website: http://research.ukzn.ac.za/Research-Ethics/