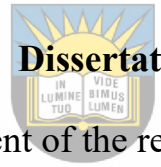
University of Fort Hare
Together in Excellence

A framework to prepare an information security awareness and training programme for a provincial government department in the Eastern Cape, South Africa

By

Zandile Potelwa

201600492



Dissertation

Submitted in fulfilment of the requirements for the degree

Master of Commerce

In

Information Systems

in the

Faculty of Management and Commerce

Of the

University of Fort Hare

Supervisor: Mr Duane Boucher

7 March 2022

Abstract

Provincial government departments do not have good audit reports on the information security section. The underlying issues are human factors associated with employee interaction with Information and Communication Technology (ICT). The problem to be addressed is how a provincial government needs to focus on employees' information security awareness so that there is a residual improvement in information security culture to realise unqualified government audits for information security.

A case study approach that focused on the provincial government departments in the Eastern Cape Province was used. The primary data was collected using semi-structured interviews containing questions related to information security awareness. Microsoft Teams was used to conduct online semi-structured interviews with 12 provincial government IT staff from two identified provincial departments. The data was analysed using thematic analysis and MS Excel for coding.

The findings then were used to determine the outcome of this study which is the framework for preparing an information security awareness programme. The outcome of the study was achieved by condensing the themes that emerged in both the primary and secondary data. The framework was then explained as a way of recommending the importance of preparing information security awareness and training programmes in changing information security behaviour. The derived artefact of this study is an information security awareness framework that can be utilised in a provincial government department to increase the awareness of information security amongst government employees. The contribution of this study is a framework based on the Protection Motivation Theory and the Organisational Culture, to ascertain employees' actions in relation to information risks and threats; requirements for preparing an information security awareness program for public sector employees and to determine the requirements to be considered when building information security culture in provincial government departments.

The proposed framework can then be used to establish an information security culture within the government departments, which will mitigate security risks and threats. The significance of this study as per the constructs of ISA and training show that it can challenge thinking of how ISA can be prepared for not only provincial government but also for state-owned entities or local government.

Keywords: Information Security; Security Culture; Information Security Awareness

Declaration

I, Zandile Potelwa (201600492), hereby declare that:

- I claim the work presented here as my own and that it has not been submitted anywhere in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognised educational institution.
- All sources used or referred to in this work have been acknowledged.
- I am fully aware of the University Of Fort Hare's policy on research ethics, and I have taken every provision to fulfil the regulations. I have obtained an ethical clearance certificate from the University of Fort Hare's Research Ethics Committee, and my reference number is the following: **BOU021SPOT01** (Attached as Appendix A).

7 March 2022

Acknowledgements

The journey towards acquiring this qualification needed extra strength from others to cheer me up along the way. Many thanks to:

- My God - the Creator of Heavens and Earth for giving me supernatural strength when I desperately needed it.

- My research supervisor, Mr Duane Eric Boucher, for your guidance, patience with me and support and encouragement.

- My family – Zuko, Mtombo, Amahle and my siblings for allowing me to be absent from your lives.

- My post-grad workshop classmates Thandie, Buli, Pam, Yoli and Cve for cheering me up and saying it is doable, and I am almost there when I doubt myself.

- Govern Mbeki Research Council and Post-Graduate Research unit for sponsoring capacitation workshops to assist in research development skills.

CONTENTS

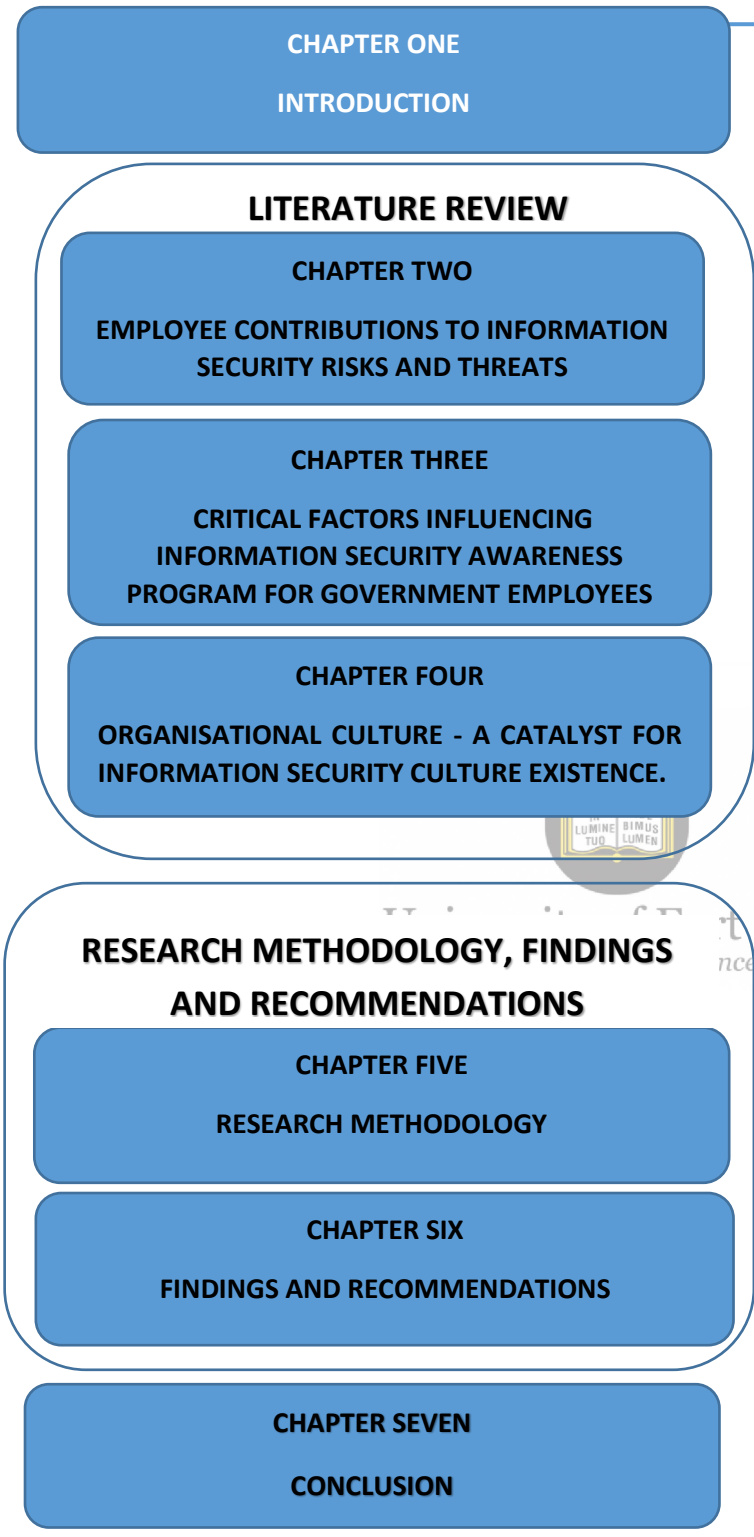
List of Figures

List of Tables

List of Key Acronyms

Acronym	In-Full	Description
ISA	Information Security Awareness	"A state where users in an organisation are aware of their security mission" (Siponen, 2000)
ISC	Information Security Culture	"A totality of patterns of behaviour in an organisation that contributes to the protection of information of all kinds" (Dhillon, Syed, & Pedron, 2016)
ISCA	Information Security Culture Assessment	An ISC assessment (ISCA) instrument assists in determining whether the ISC level of an organisation enhances the protection of information assets, thus minimising the threat to its confidentiality, integrity, and availability (Nel, 2017).
ISP	Information Security Policies	"Refers to clear, comprehensive, and well-defined plans, rules, and practices that regulate access to an organization's system and the information included in it" (National Center for Education Statistics, 2019).
MISS	Minimum Information Security Standards	"Are guidelines for the minimum information security measures that any institution must put in place for sensitive or classified information to protect national security" (Michalsons, 2017)

CHAPTER ONE: INTRODUCTION



1.1. The background of the study

Information security is the protection of the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission, via the application of policy, education, training and awareness, and technology (Whitman & Mattord, 2021). The utility of information is based on these three characteristics (confidentiality, integrity and availability). The objective of the audit process conducted for information security is to check whether government departments's information has these characteristics. The Eastern Cape provincial departments have qualified audit reports from the Auditor-General concerning information security breaches (Eastern Cape Provincial Treasury, 2016). This is the case even though government departments have information security policies to guide the security behaviour of government employees (Eastern Cape Provincial Treasury, 2016). The auditing process is performed based on set policies and governance frameworks set by an organisation or industry. An information security policy (ISP) is a document that organisations endorse to guide their workers to comply with ISPs regarding digitally stored data within the organisation's borders (Kostadinov, 2014). A significant number of security incidents are caused by a human error caused by employees when they do not conform to information security policies (Siponen, Mahmood, & Pahnila, 2014; Sherif, Furnell, & Clarke, 2016; Connolly & Lang, 2013; Van Niekerk & Von Solms, 2010). Consequently, understanding and acting on shortcomings concerning employees' awareness of ISP is essential for reducing information security incidences (Bauer, Bernroider, & Chudzikowski, 2017; Nasir, Arshar, & Hamid, 2017).

Research into employee compliance behaviour (Nasir, et al., 2017) has found that information security culture (ISC) plays a significant role in influencing employee compliance with ISPs. Information security culture has been broadly defined as the "totality of patterns of behaviour in an organisation that contributes to the protection of information of all kinds" (Dhillon, Syed, & Pedron, 2016, p.63). Alternatively, ISC was defined as: "the collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction with information assets in an organisation to influence employees' security behaviour to preserve information security" (Alhogail, 2015, p.567).

An effective ISC can help in mitigating the information security risk caused by the behaviour of employees while processing or handling information (Da Veiga & Martins, 2017). Organisational culture should promote the safeguarding of information. An ISC has to be

fostered in such a way that there is compliance to ISP by employees. By so doing, risks caused by workers' side, for example, unlawful disclosing of restricted information, wrongful usage of information, will be reduced (Da Veiga & Martins, 2015). According to Busch, Patil, Regal, Hochleitner and Fröhlich (2015), having formal, documented security policies has to be conducted first in order to instil ISC and is regarded as a good practice (ISO/IEC 27013, 2021). The ISPs define the expected security behaviour and sanctions in the case of non-compliance to ISPs, in an effort to change how employees behave towards information security (Busch, Patil, Regal, Hochleitner, & Fröhlich, 2015). Being aware that ISPs exist shows the extent workers are mindful of and perceive information security. When employees are aware of information security, ISC can develop. According to Chen, Ramamurthy and Wen (2015), if awareness of ISPs is effectively communicated, it can assist in forming up ISC since the values, mission, and vision of the organisation is clearly articulated to the employees. Herath and Rao (2009) conclude that ISP, as well as information security awareness, can assist the organisation in fostering the desired point of ISC.

Building ISC aims to improve employee behaviour with respect to information security where employees interact with information assets to protect these assets. Therefore, it is crucial to develop the ISC in organisations so that the way employees behave with information security as well as other regulatory frameworks. This is possible if the organisation assesses, monitors and influences ISC. Information security culture can then be informed by the data collected from an ISC assessment, with key focuses on programmes of training and awareness (Da Veiga & Martins, 2015). There is a need to prepare a framework for information security awareness because training and awareness assist in improving ISC and play a part in protecting information (Da Veiga & Martin, 2015; Chen, Ramamurthy, & Wen, 2015).

1.2. Problem Statement

Technical methods to provide information security have been developed and implemented, but they are not effective in ensuring ISPs compliance on their own. Therefore, it is critical to focus on issues that are not technical, such as human factors (Schultz, 2005; Metalidou et al., 2014). Research indicates that noting human-related factors is important to successfully protect organisational information assets (Alfawaz, Nelson, & Mohannak, 2010). The key focus areas when auditing information security in Government are user account management, security management, Information technology service continuity, and human behaviour. Human behaviour is the most noteworthy focus area compared to other focus areas for the past four

consecutive years (Eastern Cape Provincial Treasury, 2017; 2016; 2015; 2014; (Crossler, et al., 2018; (Lebek, Uffen, Neumann, Hohler, & Breitner, 2019). A provincial government may install security software such as network monitoring tools for efficiency or set up off-site disaster recovery sites, but if there is no ISC both at an organisational and individual level, then the security threats and risks will not be mitigated. An ISC gives direction and structure to the way humans behave when they interact with ICT to mitigate the risks related to securing information assets. Security is only possible when employees recognise, comprehend and agree with the necessary precautions (Al Hogail A. , 2015).

Eastern Cape government departments do not have good audit reports for information security (Eastern Cape Provincial Treasury, 2017; 2016; 2015; 2014). The underlying issues are related to human factors associated with employee interaction with Information and Communication Technology (ICT). ISC has significance in influencing compliance with ISPs and ICT interaction with employees. However, to foster an ISC, it is necessary to ensure there is a suitable awareness of security-related threats, together with controls, through appropriate awareness programmes. The problem to be addressed is how a provincial government needs to focus on employees' information security awareness so that there is improvement in ISC in order to realise unqualified government audits for information security. The intended contribution from the investigation of the problem is the derivation of a framework to prepare information security awareness programmes for government departments.

1.3. Objectives of the Study

This study aimed to produce a framework to be used to prepare information security awareness programmes in selected government departments. Furthermore, the presented framework will enrich the application of ISPs and thereby improve ISC. The framework was developed through achieving the following secondary objectives:

- To ascertain the processes and activities performed by employees and employers to address information security, risks and threats;
- To investigate the factors required for the preparation of an information security awareness program for public sector employees and
- To determine the requirements to be considered when building ISC in provincial government departments.

1.4. Research Questions

To address and answer the identified problem, the main research question and the sub-questions were detailed.

1.4.1. Main research question

How should the Eastern Cape Provincial Government prepare an information security awareness programme to foster an information security culture amongst employees in government departments?

1.4.2. Secondary research questions

Secondary research question 1. How do employees contribute to information security risks and threats?

The quick change towards automated government services globally led to exposing confidential information in government to possible cybercrime. Therefore information security has become a crucial issue that has to be effectively dealt with in government development (AlKabani, Deng, & Kam, 2015; Karokola, 2012). The effective management of information security in government is critical in developing successful automated government services because it boosts the confidence and trust of the citizens who use these services (AlKabani, Deng, & Kam, 2015). To mitigate security risks and to minimise information security incidents, it is critical that employees comply with information security policies (Bauer, Bernroider, & Chudzikowski 2017; Nasir, Arshar, & Hamid, 2017). To address this sub-question, strategies and guidelines to mitigate risks and reduce security threats were explored.

Secondary research question 2. What are the main factors that influence information security awareness amongst employees?

This sub-question identified factors, which are critical in conducting security awareness in the organisations. For better improvement of compliance by users, information security managers have conducted information security awareness programmes that were designed to convey information to the relevant employees (Bauer et al., 2017). Whitman and Mattord (2018) assert that if there is no program for security awareness, users may start to ignore security matters, which leads to a rise in employee failures and security threats. Somroo, Shah, and Ahmed (2016) discovered that management intervention initiatives such as the development and

implementation of an ISP and information security awareness substantially influenced the best management of information security.

Secondary research question 3. What are the requirements to consider when fostering an information security culture in provincial government?

A well-developed ISC can lead to a reduction of risks resulting from the behaviour of employees while dealing with and handling information (Da Veiga & Eloff, 2010). ISC is defined as

"attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organisation's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour (i.e. incidents) evident in artefacts and creations that become part of the way things are done in the organisation to protect its information assets" (Da Veiga & Eloff, 2010, p198).

Corris (2010); Siponen, Mahmood, and Pahnila (2014) assert that employees adhere to policies and have compliance behaviour if the organisation's executive management promotes the policies. When everyone adheres to policies and comply, compliance will automatically change into organisational culture (Corris, 2010). The mistakes that organisations make are that they regard information systems governance as part of the information technology unit and corporate governance (Corris, 2010). Organisations do not understand that information system has to be integrated into the organisational culture (AlKabani, Deng, & Kam, 2015; Corris, 2010; Connolly & Lang, 2013).

1.5. The significance of the study

The management of information security is crucial for government enterprises if the public sector aims to successfully implement e-government developments or similar that have the trust of its stakeholders to provide secure information (Karokola, 2012). Parsons, McCormac, Pattinson, Butavicius, and Jerram (2016); De Lange, Von Solms, and Geber (2015) support this statement by saying that it is critical to maintaining a significant amount of electronic data, for this reason, the management of information security is very important for public sector organisations who are custodians of large amounts of information. AlKabani, Deng, and Kam (2015) also agree and suggest that establishing ISC is necessary to reduce future security risks and threats to information assets.

To address a gap in adopting ISC in government, Alnatheer and Nelson (2009) suggest conducting information security awareness and training for all employees to incorporate ISC into the organisational culture. Information security awareness enables improvement in information security behaviour and ensures that employees comply with ISPs (Bauer, Bernroider, & Chudzikowski, 2017; AlKabani, Deng, & Kam, 2015). The reason for targeting the provincial government as an organisation in this study is because the Government keeps critical information for the citizen of a country, such as health, education, finance and security. Therefore, it becomes critical to safeguarding the information assets of the state from security threats in the relevant departments. The intended result and benefit of this study would be that government managers can mitigate information security risks and threats in their workplace guided by a framework for an information security awareness programme.

1.6. Literature and Theory

Theories give both a framework to critically understand facts and a foundation for allowing how what is not known can be structured (De Benetti, 2014). Therefore, theories emphasise the rationale for research (Silverman, 2000). This study used Internet resources and government-related documents as secondary data. The primary data collection derived was detailed under section 1.7 - Research Design. In this section, the underlying theories guiding this study were introduced; thereafter, a brief literature review from secondary data was provided to contextualise the study.

1.6.1. Theoretical Perspective

This research was guided by the Organisational Culture Theory (OCT.) (Hogan & Coote, 2013; Schein, 2004) and the Protection Motivation Theory (PMT) (Boer & Seydel, 1996). The OCT framed the discussion of the organisational constructs, whereas the PMT was applied to individuals in the organisation. Each of the theories was briefly discussed.

1.6.1.1. Organisational Culture Theory (OCT)

Schein's Model of Organisational Culture Theory (OCT) (Schein, 2004) was used in this study as the foundation to improve an ISC amongst organisational employees. Schein (2004) asserts that there are three echelons of organisational culture: artifacts and symbols, espoused values, and basic underlying assumptions (*cf.* Figure 1.1).

Artefacts and symbols denote the outward of the organisation. They are the noticeable components within the organisation, for example, logos, architecture, organisational structure, processes and corporate clothing. Therefore, these are not only noticeable to the employees but observable and noticeable for people outside the organisation. They serve to create a corporate identity. Espoused values relate to rules of conduct, values and standards. They involve the manner the organisation communicates its strategies, objectives, or the organization's public statements of identity.

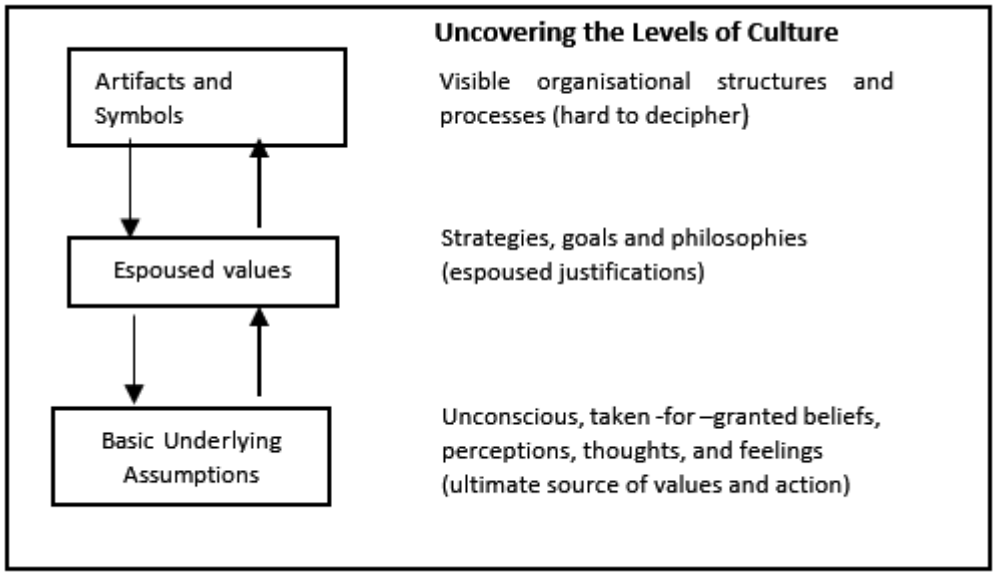


Figure 1: Schein's three layers of organisational culture (Schein, 2004)

Challenges may arise in a situation where espoused values of the leadership are not aligned with what is deemed to be the organisation's simple norms. These basic norms are usually shared by groups, are encapsulated within the culture of the organisation and are easily noticed and are done effortlessly by employees. These norms are usually those philosophies or views which employees, as a collective, do not doubt or dispute, and as such, becomes hard to change. Assumptions come into effect after repeatedly validating and reinforcing values. Therefore, assumptions control the behaviour of a group, its views, opinions, and approaches to a situation (Schein, 2004).

In this study, the OCT assisted in pointing out the importance of establishing organisational culture as a necessity for effective ISC because organisational culture affects how employees behave and the actions of the whole organisation (Tang, Li, & Zhang, 2016). According to Tang et al. (2016), information security practices should be reinforced and guided by its

organisational culture. The reason is that a strong organisational culture focused on information security directly influences employees' behaviour in conforming to IS standards and policies in government (AlKabani, Deng, & Kam, 2015).

The development of organisational culture can provide inputs into the processes to follow to develop an ISC (Da Veiga & Martins, 2015; Schlienger & Teufel, 2003; Zakaria & Gani, 2003). An ISC develops because there is a security behaviour of employees, so is an organisational culture, which develops because there should be a certain way of how employees should behave in an organisation (Da Veiga & Eloff, 2010).

An organisational culture forms up when an organisational top management crafts organisational vision and strategy, which is demonstrated in policy frameworks, such as espoused values (Zakaria & Gani, 2003). The way employees behave will show in the policy frameworks, and finally, the culture of the organisation is formed, which will include policies, strategy, vision and what employees experienced when actually implementing these, such as the basic underlying assumptions. It was, therefore, necessary to have a better understanding of what motivates individuals towards the protection of information.

1.6.1.2. Protection Motivation Theory (PMT)

The PMT has an assumption that an employee is familiarised with new concepts, after which the employee would evaluate that concept and then make a conclusion to a protective response (Clubb & Hinkle, 2015). PMT is premised on the view that the behaviour of individuals can be shaped and is predictable (Boer & Seydel, 1996). According to Rogers (as cited in Boer & Seydel, 1996), PMT is a theory of persuasive communication that emphasises the cognitive processes to mediate behavioural change. Employees do not simply adhere to information security regulatory frameworks, and that causes security risks and threats (Siponen, Mahmood, & Pahnila, 2014). The PMT can be applied to persuade individuals in the organisation of the importance of complying with ISPs (Bauer, Bernroider, & Chudzikowski, 2017). Employees' compliance with information security standards is crucial for the reduction of information security incidents (Bauer et al., 2017). Connolly and Lang (2013) support the idea of employee compliance as a necessity to promote an ISC where employee behaviour complies and assists the organisation in preventing information security breaches that are human-related.

The PMT can be utilised to arrive at common themes which focus on changing employee behaviour using its four factors. These factors are (Wu et al., 2005, p.127-128) :

> "(a) the perceived severity of a threatening event (e.g. risks of intrusion into sensitive government information by hackers), (b) the perceived probability of occurrence or vulnerability (in this example, the perceived vulnerability of information assets risk attacks), (c) the efficacy of the recommended preventive behaviour (the perceived response efficacy), and (d) the perceived self-efficacy (i.e., the level of confidence in one's ability to undertake the recommended preventive behaviour)".
>
> The benefit of compliance is shaped by intrinsic benefit, the safety of resources and rewards, while the cost of compliance is shaped by work impediment. The cost of noncompliance is shaped by intrinsic cost, vulnerability of resources, and sanctions (Bulguru, Cavusoglu, & Benbasat, 2010).

These four factors made a contribution to the successful development of the information security awareness programme (training) that resulted in a change in the ISC (behaviour).

1.6.2. Empirical Perspective

An outline of the main content areas that were used to address the main research question (*cf.* section 1.4.1) follows.

1.6.2.1. Compliance to ISPs and procedures/regulatory framework

The main reason for a policy in an organisation is to shape and define the decisions, behaviour and actions of the employees to articulate behaviour that is acceptable and not acceptable (Whitman & Mattord, 2021). Irrespective of the organisation, it is imperative that users comply with ISPs to avoid negative implications for the organisation (Bauer et al., 2017). In support of this notion, Siponen, Mahmood and Pahnila (2014) argue that the greatest threat to information security is employees' non-compliance to ISPs. Nasir, Arshar and Hamid (2017) conclude that when employees adhere to organisational ISPs, the mitigation of information security risks occurs.

1.6.2.2 Organisational culture and Information security culture (ISC)

It is necessary that an organisation establishes an organisational culture for effective ISC because organisational culture affects how employees behave and the actions of the whole organisation (Tang, Li, & Zhang, 2016). A strong organisational culture on information security directly influences employees' behaviour in conforming to IS standards and policies in government (AlKabani, Deng, & Kam, 2015). To ensure that information security is incorporated into the culture of the organisation, employees should be familiar with how to protect information as one of their everyday activities (Thomson, Von Solms, & Louw, 2006). Van Niekerk and Von Solms (2010) state that employees pose a significant threat to information security, and therefore it is crucial to have an existing ISC as a sub culture of organisational culture. Organisational employees have to be trained as to their roles and responsibilities with respect to the protection of information assets, or the organisation cannot ensure the protection of the integrity, confidentiality and availability of the organisation's information (Thomson, Von Solms, & Louw, 2006). It is the responsibility of the senior management of the organisation to foster organisational culture (Alnatheer & Nelson, 2009). Previous studies have shown a strong link between organisational culture and ISC (Da Veiga & Martins, 2017; Connolly & Lang, 2013; Nasir, Arshar, & Hamid, 2017). Therefore, it is important to create an ISC in order to achieve successful security compliance of the organisations.

1.6.2.3 Information security awareness (ISA)

By definition, "information security awareness is a state where users in an organisation are aware of their security mission" (Siponen, 2000, p. 31). Van Niekerk and Von Solms (2010) state that if employees do not cooperate and have no knowledge, there can be misuse and misinterpretation of information security policies and procedures. ISO/IEC 27013 (2021) suggests that organisations conduct an information security awareness campaign to make sure that organisations adequately know about information security. Van Niekerk and Von Solms (2010) assert that in order to create security awareness, it is necessary to make information security a normal activity of every employee performing their job. The most successful way for an organisation to preserve its data and make sure that it complies with ISPs is when the top management encourages security in their day-to-day actions (Corris, 2010; Thomson, Von Solms, & Louw, 2006; AlKalbani, Deng & Kam 2015). Previous research indicates that information security awareness can lead to improved information security behaviour and ISP

compliance (Bauer, Bernroider, & Chudzikowski, 2017). AlKalbani, Deng, and Kam (2015) found that information security awareness has a significant impact on information security compliance.

Therefore employees in public administrations must have an awareness of the security risks and cyber threats they are confronted with, how they should be responsible with security policies they use and the guidelines to deal with risks, as well as the repercussions of information security breaches (AlKalbani, Deng, & Kam, 2015; Thomson, von Solms & Louw, 2006). AlKalbani, Deng and Kam (2015) conclude that three key aspects that are crucial to forming the ISC are: management commitment, accountability, and ISA. Da Veiga and Eloff (2010); Van Niekerk and Von Solms (2010), as mentioned by Al Hogail (2015), suggested that organisations should prepare an awareness program in order to instil ISC. Al Hogail (2015) emphasized a need to develop a detailed framework to instil and evaluate an organisational culture that is security-aware and recommended a detailed Information Security Culture Framework (ISCF).

1.7. Research design

The research design is a master plan or the logical approach for an investigation that provides direction on how the research is to be conducted (Thomas, 2010). It includes the entire strategy that researchers decide on put together the diverse sections of the study such that the study is logical and coherent to ensure that researchers may answer the research problem (Sestak & Sestak, 2010). The following Figure 2. below maps out the research process followed during the data collection and analysis process in this study.

The research design comprises the research paradigm that the study will use, the research method, the data collection method, and the sample and analysis methods to be employed, all of which are discussed in this section.

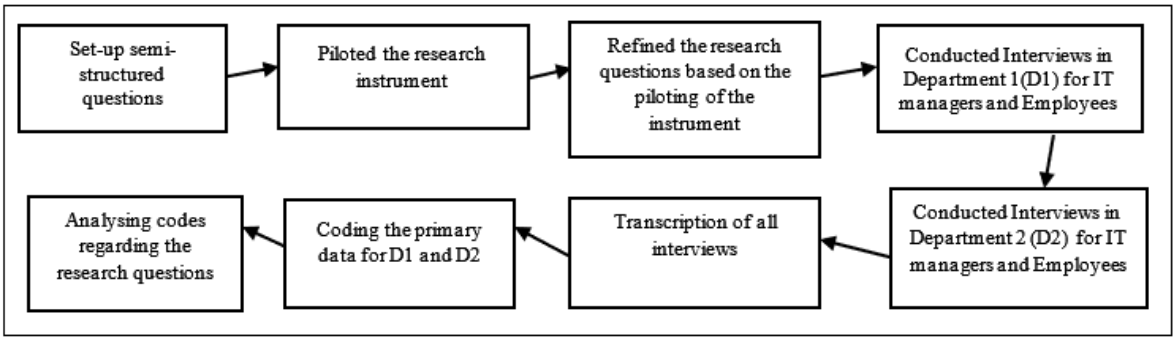


Figure 2: The Data collection and Data analysis process (adapted from Bauer, Bernroider, & Chudzikowski, 2017)

1.7.1. Research Paradigm

The interpretive research paradigm (interpretivism) was used as the underlying philosophical paradigm for this study in order to facilitate the exploration of the given setting(s) (*cf.* Section 5.2; Table 6). Interpretivism supports the assimilation of understanding by the researcher and the dissimilarities between humans in their roles as social actors (Saunders, Lewis, & Thornhill, 2009). The choice of this philosophy allowed the researcher to gain a deeper understanding of the information security awareness context (examples provided in brackets) by acquiring knowledge from humans (i.e. employees), through their lived experience (i.e. how the employees perceive information security), and their interactions (i.e. employee behaviour) with the environment (i.e. information assets of the government) (Creswell, 2014). The interpretive philosophical paradigm factors in the acquisition of knowledge by the researcher in that a researcher conducting a qualitative study needs to be aware of their own bias when arriving at the solution to the identified problem.

1.7.2. Research Method

A qualitative approach as the data collection method was used. Qualitative research sought to achieve a deeper understanding of the problem being investigated to produce new findings (Flick, 2018). The qualitative research method makes use of various techniques, for example, interviews, focus groups, and open-ended questionnaires, which provide rich interpretive data from the participants in order to understand the underlying reasons, motivations and opinions behind the phenomenon under investigation (Barbie & Mouton, 2001). Therefore, a qualitative research method was to better understand employees' thoughts and motivations demonstrated

towards information security in order to better understand how an information security awareness programme could be prepared for use in government departments.

A case study design was used as it investigated the understanding of information security in the selected two departments. Together they formed a sample of the representative of Departments in the Eastern Cape Provincial government. A case study is defined as an empirical inquiry that explores a current phenomenon (the 'case') comprehensively and as they actually occur (Yin, 2018; Meyer 2015). Meyer (2015) states that the primary aim is to have a deeper understanding of the case rather than the testing of the theory-driven claims. Meyer (2015) states that case study data might be coming from a variety of sources, for example, direct observation, interviews, documents, archived documents or participant observation.

1.7.3. Data Collection

The secondary data discussed in the literature chapters was complete by conducting online searches via research search resources / databases such as GoogleScholar, ACM Digital Library, Emerald Insight, Science Direct and Mendeley for articles and relevant reference material. The search phrases used included: "information security culture", "organisational culture", "information security policies", "information security risks and threats", and "information security awareness". The writeup of the literature based on the sources identified informed the development of the research instrument and the discussion of findings.

This research project collected primary data through semi-structured interviews with government employees who are custodians of information assets. Interview questions were about information security risks and incidences, and information security awareness. According to Bryman and Bell (2011), semi-structured questions allow the participants to give in-depth information about the phenomenon under investigation. The data (constructs of importance) that were collected include information security policy awareness, perceived security risks, security incidences, information security training or awareness and behaviour reactions towards security. The questions for the semi-structured interviews were prepared and framed through the use of the constructs which appeared in the OCT and PMT.

1.7.4. Data Sampling, Analysis and Validation

The following section provided a brief discussion of the data sample size, the analysis technique used to analyse the data, and how the data was validated.

1.7.4.1 Data sample

Qualitative studies do not have an agreed sample size; subsequently, a researcher can explore different guidelines that can be used (Creswell, 2014; Simon & Goes, 2012). The sample size identified for the study was 12 participants. The sample size was small with the intent to gain a holistic view of the current phenomenon, ISA. Two Provincial Departments were identified to compare and contract any significant differences within the current operations and policies of the Departments with respect to ISA. In total, eight IT support employees (four operational employees per department) and four IT managers (two IT managers per department) were identified and are detailed in Table 1. Given the COVID pandemic and lockdown restrictions the identified participants were only able to interact virtually with the researcher.

Table 1: Study participants

Cases	**Participants**		
Department	**IT Managers**	**Employees**	**Total**
Health	2	4	6
Office of the Premier	2	4	6
GRAND TOTAL	**4**	**8**	**12**

The purposive sampling technique was used as the sampling method of this research project. Barreiro and Albandoz (2001) state that the purposive sampling technique seeks to gain deeper insights into the phenomenon studied rather than the issue of generalisation. The reasons for opting for the purposive technique for this study were the proximity of the participants to the researcher and shared employee characteristics among the participants that fitted what the study sought to understand.

According to Saunders, Lewis, and Thornhill (2009), purposive sampling permits the researcher to critique findings from a selection of cases to answer the research question and to solve the problem identified. Purposive sampling is mostly applied when dealing with case study research as well as in cases where the researcher intends to choose cases that are particularly informative (Saunders, et al., 2009).

1.7.4.2 Data analysis

The data gathered from semi-structured interviews with employees and managers were analysed to categorise the responses from participants against identified themes from literature and the two underlying theories of the study. Thematic analysis was the method of analysis used for the study. According to Braun and Clarke (2014), thematic analysis is used mostly in

qualitative studies and assists in examining, pinpointing, and recording themes within data. Themes are viewed as the patterns that are found across data sets and are of importance in describing a phenomenon (Fereday & Muir-Cochraine, 2006). Furthermore, the themes are connected to a specific research question that makes up the objectives of the phenomenon under investigation (Fereday & Muir-Cochrane, 2006). These themes guided the researcher in developing the intended framework to prepare information security awareness programmes in government departments as a means to foster an ISC to mitigate security threats.

The primary data collected from respondents was anonymised as far as possible by referring to the departments as D1and D2. Each respondent will be afforded a number R1, R2 …Rn.

1.7.4.3 Data validation

Data validation gives the key concepts that establish the quality and trustworthiness of the primary data. Unlike the quantitative method that explains these aspects using internal and external validity, reliability and generalizability terms, qualitative validation focuses on the credibility, transferability, dependability, and confirmability of the analysed primary data.

Credibility, according to Merriam (as quoted by Shenton, 2004), is the qualitative investigator's counterpart that answers the question, "How congruent are the findings with reality?" (p.64). To make sure that this study maintains credibility, after the questionnaire, the researcher will take the transcript back to interviewees to verify the correctness of the data.

Transferability, according to Shenton (2004), demonstrates that the findings of the study at hand can be used in similar environments. The ability of the researcher to evaluate whether results can be transferred to another environment that is similar is determined by the selection of participants and findings, as well as a detailed description of the research. Making use of a multiple case study approach will enable the transferability of findings.

Dependability relates to how similar results would be received if the researchers repeat the study (Creswell, 2014). To tackle the issue of dependability completely, the researcher should report the processes performed in the study in a detailed manner so that other researchers in the future can repeat the study and get similar results. The research process followed in this study will therefore be explicitly detailed.

Confirmability relates to the qualitative researcher's comparable concern about fairness (Shenton, 2004;). The researcher must take precautionary measures to ensure the results of the study are the outcomes of the experiences and ideas of the informants and not the researcher's

traits and inclinations of the researcher. Miles, Huberman and Saldana (2018) state that what is crucial for confirmability is the extent to which the researcher can acknowledge his or her own biases. Firstly is to acknowledge that self-bias is possible even prior to data collection. To do this, the researcher can ask the following questions:

- Who are the respondents? Do they have characteristics that are likely to be prone to response bias?
- What methods are used to collect data? Unclearly phrased questions and few options wherein the respondent can cause an unexpected pattern of unwanted responses, for example, extreme, midpoint or consistency bias effect.
- What is the context in which data are collected? In the circumstances with external variables, for example, scheduling and time pressures associated with the collection, interruptions because of noise or lighting or temperature can result in response bias that can affect the results (McCue & Tartaglia, 2010).

1.8. Delimitation of the Study

This exploratory study was limited to investigating the factors that influence ISA programmes, to ascertain those processes and activities performed to address security risks and threats, and to investigate what is required in order to foster an ISC for government employees for provincial government departments in the Eastern Cape. The study was limited to the available access to IT support employees and IT Managers from two provincial government departments based in Bhisho in the Eastern Cape, South Africa. During the time of data gathering the provincial staff were working remotely due to COVID restrictions, which limited accessibility to staff. Further study on the information security awareness phenomenon with respect to general employees in a government context would require a larger sample size to refine the framework provided in this study.

1.9. Ethical Considerations

The necessary ethical clearance approval process was sourced through the University of Fort Hare Ethics Committee (UREC), as it was compulsory in order to undertake this study. The clearance approval certified that the researcher agreed to conduct the study ethically and ensured the protection of rights of the participants in the research. Saunders et al. (2009) quotes the following factors for consideration when collecting data "(1) preservation of the confidentiality of data and anonymity of the participants; (2) notifying the participants of the

voluntary nature of the study and their privilege to withdraw or participate in the study, and (3) participants must be informed of how the data collected will be used as well as the third parties who might have access to the data" (p.183). The researcher was obliged to ensure that all these factors relating to ethical standards were fulfilled when conducting a study. Therefore, the researcher ensured that she abided by the above-mentioned factors during the entire process of the research study.

Gatekeeper permission from the case sites (selected government departments) was requested and granted by the Heads of the two departments before the interviews were conducted, and all identified participants (employees) were given the opportunity to withdraw their participation from the study if they felt in any way uncomfortable with the research study and the data collection process.

1.10. Overview of the Rest of the Study

Chapter 1 is made up of the proposal, which is the introductory chapter of this research. The proposal gives an overview of what the study seeks to achieve. In this chapter, the researcher presents a brief background of the study and also identifies the problem in the form of research questions. Afterwards, three sub-questions that will help the author to answer the main research question are proposed. Chapter 1 also discusses the significance of the study and how it can add value to the existing body of knowledge in the subject area.

Chapter 2, the first literature chapter, will introduce the processes and activities performed by employees to address the information security risks and threats**.**

Chapter 3, the second chapter of the literature review, will introduce the factors which are critical in influencing an information security awareness program for government employees. **In Chapter 4**, the last literature chapter will determine the requirements to be considered when building ISC in provincial government departments.

Chapter 5 discusses the research methodology and research design. This includes the research paradigm, data collection methods and data analysis procedures.

Chapter 6 discusses the findings resulting from the primary data collected for the research study, as well as the contributions which is a solution to the research problem by presenting a framework to prepare ISA and training programme**.**

Chapter 7 concludes the whole research project by highlighting the significance of the study, outlining the unique contribution made by this study, and giving suggestions for future research.

CHAPTER TWO: EMPLOYEE CONTRIBUTIONS TO INFORMATION SECURITY RISKS AND THREATS

2.1. Introduction

Organisations use technology-based means to reduce threats to information security (Alavi & Islam, 2016; Arbanas, Spremic, & Hrustek, 2021). Organisations should have information security policies (Hina & Dominic, 2018) and Security Education, Training and Awareness programs (Alshaikh, Maynard, Ahmad, & Chang, 2018). These are non-technical means to prevent security breaches that employees cause. Employees are the ones who cause many challenges in information security (Astakhova, Botha, & Herselman, 2020; Thomson & Van Niekerk, 2016; McIlwraith, 2016; Parsons et al., 2017); hence organisations are focusing on employees' information security awareness and behavioural reasons for the security breaches as well as instilling a security culture. When employees (the management and users) undergo appropriate training and awareness sessions about the organisation's threats, employees can be instrumental in mitigating security risks (Wiley, McCormac, & Calic, 2020).

The chapter is divided into subsections that will assist in gaining an understanding of how employees can assist in mitigating security risks and threats. We begin by defining information security, which is the underlying theme of this study. In addition, the chapter focuses on understanding the principles related to predicting and shaping employee behaviour so that there is compliance with information security policies. The Protection Motivation Theory is the basis of the discussion of this chapter.

2.2. Defining information security

Paliszkiewicz (2019, p.1.) defined information security as the "protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability".

The definition of information security includes safeguarding information as well as its crucial elements, comprising the systems and hardware that use, store and transmit the information, broad areas of information security management, data security and network security (Koohang, Anderson, Nord, & Paliszkiewicz, 2019). The Committee on National Security (CNS) model emanated from the confidentiality, integrity, and availability (C.I.A.) triangle concept developed by the computer security industry (Whitman & Mattord, 2018). The C.I.A. is founded on the three qualities of information that make it valuable to the organisation: confidentiality, integrity and availability (Whitman & Mattord, 2018). Confidentiality of

sensitive information seeks to prevent disclosure of information to unauthorized users. Integrity ensures that data cannot be modified without authorization (Whitman & Mattord, 2018). Availability ensures that information is available to authorized users when required (Whitman & Mattord, 2018). Information security has become more critical in today's information security age as information technology develops because information resources' privacy and other security concerns arise (Gebrasilase & Lessa, 2017).

In ensuring the security of information resources, technological means, for example, setting up strong passwords or installing firewalls, may work to some extent (Whitman & Mattord, 2018). However, many information security challenges do not emanate from technological causes but are caused by other employee actions (Crossler et al., 2018; Lebek, Uffen, Neumann, Hohler, & Breitner, 2019). Information security incidents caused by users are either intentional or unintentional behaviour such as carelessly managing information, browsing websites that are not secured, or data practices that are not secure (Siponen & Vance, 2016). For that reason, it is argued that employees should be central to an organisation's information security defence system (Gebrasilase & Lessa, 2017). Human error, such as accidents, employee mistakes, and failure to follow policy, is ranked the top 12 threats to defend or react to in the 2017 ranking survey (Whitman & Mattord, 2018). In the information security environment, it is critical to apply various security approaches to mitigate the risk of information security threats.

2.3. Managing security risk

The International Standard, ISO31000 (2018), defines information security risk as a emanates from two aspects, namely: probability and consequences. ISO31000 (2018) examines the following two issues: the likelihood of a certain information security event in the future and the effects this event will bring about or the outcome if it eventually occurs. Information security risks are identified when possible security threats have emerged which can exploit vulnerabilities of information assets and therefore can be a reason for harming an organization. An Ernst and Young (EY) (2019) survey on information security stressed that study participants viewed vulnerabilities and information security threats mainly to be high because of obsolete information security controls. The survey highlighted negligent or unaware employees and unauthorized access as one of the causes. Shamala et al. (2017) suggest that the organisation selects applicable measures, effectively reduce information threat, and, most importantly, specify appropriate controls to reduce or eliminate the risks.

When an organisation is assessing its security risk, risk analysis is critical and is the first step that involves identifying valuable information assets of the organisation and their vulnerabilities, exposing threats that may exploit those vulnerabilities and may cause risks to the organisation, including estimating the damage that may be suffered as well as the possible losses caused by these risks (Shameli-Sendi, Aghababaei-Beazegar, & Cheriet, 2016). That amount of risk the organisation is willing to accept is called risk appetite (Whitman & Mattord, 2018). We explain the nature of security risk by defining the following concepts: a threat, a threat agent, a vulnerability and controls.

2.3.1. A threat

A threat is a category of objects or people that pose a danger to an information asset. According to Sarala, Zayaraz, and Vijayalakshmi (2016), an organisation must protect information systems from being misused by threats that exploit their vulnerabilities because that can cause reputational damage to the organisation. Human error or failure (such as accidents, employee mistakes or failure to follow a policy) is one of the twelve general categories of threats to information security (Whitman & Mattord, 2018). Human errors are all actions carried out without any malicious intentions by an authorised user. Errors occur when employees use information, and similar mistakes happen when employees do not follow the institutionalised policy. Giandomenico and De Groot (2018) assert that threats which come from employees are not easy to prevent.

To mitigate the risks and employee threats from malicious intent, it is critical to have an all-inclusive security approach that deals with the intentional and unintentional threats (Giandomenico & De Groot, 2018). Shameli-Sendi et al. (2016) state that the ISO/IEC7498-2 outlines the main security threats as corrupting or modifying information, stealing, removing, or losing data, disclosing information and interrupting services.

2.3.2. A threat agent

Jouinia, Rabaia, and Aissa (2018) define a *threat agent* as a person or entity that inflicts the threat on a particular system's asset, classified as either human, technological or unexpected natural cause. One of the most significant threat agents to an organisation's information security is the workers because of their close proximity to the information (Whitman & Mattord, 2018). For example, employees are the threat agents for the threat known as human

error. Employee mistakes can quickly reveal classified data, entry of erroneous data, accidental deletion or modification of data storage in unprotected areas, and failure to protect information (Whitman & Mattord, 2018). To leave information that is regarded as classified in public and not protected spaces is rates in the same manner as a person seeing to as much a threat as a person who directly seeks to wrongfully use that information because vulnerability can be created by negligence which opens chances for the attacker of information assets (Whitman & Mattord, 2018).

Kraus (2018) adds that shared and weak passwords on systems within the organisation cause risks which are not easy to audit. Spacey (2016) supports this statement by saying that password violations are among the most frequently mentioned information security failures. Even though there are security policies in place, organisations are challenged to prevent password breaches. Kraus (2018) stressed that the most significant information security risk directed to organisations is posed by its employees.

Kraus (2018) asserts that when employees send unintended email files, overshare on social media, or lose a laptop or USB drive, they place an organisation's information at risk due to their negligence. Barker (2018) adds that employees not only know what data exists in an organization, but they also have a good idea as to how it is stored. Therefore if an organisation lacks robust security mechanisms, a resentful employee can intentionally share that information with a third party.

Giandomenico and De Groot (2018) warn that if an employee from a department takes their laptop to a restaurant where there is Wi-Fi, uses that Wi-Fi, and is not security conscious, a hacker might connect to that employee's device, which will make it is easy for the hacker to access the organisation's system. Hence, it is critical to formulate, maintain, and review the organisational information security policy to create awareness among employees and mitigate security risk (Lois Barker, 2018).

2.3.3. A vulnerability

Spacey (2016) defines *vulnerability* as a potential weakness in an asset or defensive control system that risks an organisation. Spacey (2016) asserts that to manage the security risks, it is

vital that the organisation understands the vulnerabilities, whether through current employees or former employees.

The vulnerability arises when current employees (Spacey, 2016; Whitman & Mattord, 2018; Sohrabi Safa, Von Solms, & Furnell, 2016):

- interact socially with customers;
- have work discussions in public areas;
- take office data out of office;
- install unapproved software and other applications;
- remove or disable security tools;
- allow unofficial people to enter the offices (tailgating),
- open spam emails;
- connect private unofficial devices to the organisation's networks;
- write down passwords and confidential information, lose security gadgets such as identification cards; and,
- are purposely absent from information security awareness training initiatives.

Vulnerability also occurs when *former employees* (Spacey, 2016; Whitman & Mattord, 2018):

- work for the organisation's competition;
- retain the organisation's data and access authorisations; and,
- share information with third parties about the former employers' security protocols.

Organisations can identify vulnerabilities from their IT audit reports or previously analysed risks vulnerability testing databases (Shameli-Sendi, Aghababaei-Beazegar, & Cheriet, 2016).

2.3.4. Controls

Controls are any security mechanisms, policies and procedures that can mitigate the risk or eliminate vulnerabilities (Whitman & Mattord, 2018). An organisation with no password reset vulnerability, for example, might want to put a defence control strategy in place, which includes applying information security policies, education and training, or using security technology. According to Sarala et al. (2016), the organisation should have an information security officer responsible for identifying proper controls for mitigating the information security risks that might occur in the organisation. The information security officer needs to consider the risks to be mitigated, its impact concerning benefits to the organisation, and how much it costs the

organisation to implement the security controls. Sarala et al. (2016) assert that selecting the controls must be done such that the cost of the chosen controls have to be within the budget limits of the organisation and should not be above the losses incurred by the organization.

The relevant risk control strategy is applying a security policy as the first line of defence towards security risks and threats. The following section will discuss information security compliance, the importance of information security policy, and the employees' motivation towards security policies compliance.

2.4. Information security compliance

Organisations find it challenging to implement ISPs, yet these documents provide organisations with rules, explain responsibilities, and sanctions for non-compliance to information policies. To enable compliance with security policies, organisations should understand what motivates employees to comply or not to comply with information security policy because employee behaviour is sustained and guided by their motivation. The following section discusses the importance of complying with ISPs and the Protection Motivation Theory as it explains what is motivating or not motivating employees' behaviour to comply with ISPs.

2.4.1. Information Security Policy

Aloitabi, Furnell, and Clarke (2016) argues that failing to comply with information security policy is a serious challenge that the organisation faces. Establishing a sound security policy is one of the principles for securing information technology systems (NIST Special Publication 800-37, 2018; Whitman & Mattord, 2018). The best security program should start and finish off with a security policy. Safa et al. (2016) assert that effective ISPs will assist employees in understanding what the organisation regards as acceptable and responsible behaviour of information resources and help create a secure information environment. An information security policy is intended to compel every employee to behave so that they safeguard information assets.

Employees must comply with ISPs to minimise information security incidents (Bauer, Bernroider, & Chudziwoski, 2017). Bauer et al. (2017) noted that security policies are the cheapest controls to implement; however, problematic to execute correctly. Aloitabi et al. (2016) mentioned that not complying with ISPs is mainly an employee challenge and not a technological challenge. Aloitabi et al. (2016) further state that employees can be categorised

into three types of behaviour when non-complying: malicious behaviour, negligent behaviour, and unawareness. *Malicious* non-compliance intends to bring harm to the information assets of the organisation. In contrast, *negligence* is to violate an organisation's security policy rather than damage the organisation. Lastly, and the third way of not complying happens because of *unawareness*, whereby employees are unaware of how important information security is for the organisation or that they exist.

Another challenge with ISPs is that organisations are not reviewing and updating their ISPs to keep them current (Cram, Proudfoot, & D'arcy, 2017). Furthermore, Aloitabi et al. (2016) discovered that it could be difficult for organisations to design and manage security policies that satisfy all the critical requirements. Additionally, organisations are not making their staff aware of updates to policies or not communicating them in the first place to reduce security risks (Hwang, Wakefield, Kim, & Kim, 2021).

Applying a policy is one of the defence control strategies to reduce the security risks (Whitman & Mattord, 2018). A policy defines the 'do's and the 'don'ts', the sanctions for non-compliance with a policy (Whitman & Mattord, 2018). An (ISP) explains the rules for protecting the organisation's information assets. It allocates duties to the different security areas, such as system administration, maintenance of the information security, and users' practices and duties. Finally, the ISP addresses legal compliance. According to NIST Special Publication 800-37 (2018), an ISP manages compliance by assigning responsibilities and specifying penalties and disciplinary action.

It is also critical to understand the motivation of employee compliance. Therefore, the following section discusses what motivates employees to abide by ISPs by considering the Protection Motivation Theory constructs.

2.4.2. Protection Motivation Theory

According to Mamonov and Benbunan-Fich (2018), the Protection Motivation Theory (PMT) presents the premise of exposing a person to persuasive messages aimed at scaring them through communicating terrible consequences of non-adherence to recommendations as a way to motivate behaviour change effectively. An everyday example is the health warning labels on cigarette boxes to encourage individuals never to smoke or stop smoking. The PMT presumes that behavioural intentions affect behaviours, which can be affected by perceptions

of perceived threat severity, individual vulnerability, general self-efficacy, and the specific response self-efficacy (Mamonov & Benbunan-Fich, 2018). The premise of PMT is directly applicable in the application of organisational information security management with employees.

Employees, more than technology, are the main reason for information security breaches. Therefore, managers who desire to safeguard information systems have to grasp how to motivate employees to behave securely (Menard, Bott, & Crossler, 2017; Abawajy, 2018; Arachchilage & Love, 2016). Directing action through motivation has been empirically tested in multiple disciplines to be effective (Menard et al., 2017). Motivation has been shown to have significant effects on affective, cognitive and behavioural elements, and these elements are also critical variables in explaining behavioural information security research (Menard, Bott, & Crossler, 2017). Chen, Wu, Chen, and Teng (2018), when studying information security, have discovered that the means of stopping employees from being negligent and being in the insider breach is by gaining knowledge of the factors affecting how employees behave towards ISP compliance.

Their findings (Chen et al. 2018) suggest that the organisation's response cost of informally imposed sanctions to employees is more effective to influence the perceptions of employees to comply with ISPS than formally imposed sanctions. Response cost is one of the critical principles of the PMT (*cf.* Section 1.6.1.2.).

The PMT is based on the notion that what motivates employees to protect information assets comes from a perceived threat of complying or not complying and a need to avoid a potentially harmful consequence. Motivation, therefore, stimulates and guides activity and may encourage employees' compliance with ISPs and take other actions to safeguard information.

The constructs of the PMT that are applicable for this study are:

a) the perceived severity of a threatening event,
b) the perceived probability of occurrence or vulnerability,
c) the efficacy of the recommended preventive behaviour, and
d) the perceived self-efficacy (i.e., the level of confidence in one's ability to undertake the recommended action).

Each of these is briefly discussed in the context of Information Security in a government department.

Peceived threat severity is the employee's opinion of how serious that particular threat is. For example, a department might want to discipline any employee who violates information security policies, or the department might terminate all employees who repetitively violate information security policies (Chen et al., 2018). Perceptions of an employee toward information security are influenced by evaluating two cognitive-mediated appraisals: threat appraisal and coping appraisal (Hassandoust & Techatassanasoontorn, 2020). Threat appraisal is how the employees perceive the severity of a threatening event (e.g. risks of intrusion into sensitive government information by hackers). Coping appraisals is the level of confidence in employees' ability to undertake the recommended preventive behaviour

The perceived probability of occurrence or vulnerability is the extent to which an employee thinks he is vulnerable to a specific threat. For example, the employee's perception of the likelihood that he might be found violating the information security policy of the department (Menard, Bott, & Crossler, 2017).

The efficacy of the recommended preventive behaviour (Response Efficacy). After the employee has analysed that there might be a threat, the employee will assess any coping mechanisms available. Response efficacy refers to how an individual perceives that recommended response addresses the threat at hand, for example, following the security policy (Menard, Bott, & Crossler, 2017). Changing and maintaining strong and unique passwords responds to reducing the threat of identity theft.

Perceived Response Costs are extrinsic or intrinsic personal costs of doing the suggested behaviour. Employees may understand response costs in various ways, such as time, money, or effort. An employee would think adopting security technologies or practices specified in the information security policies hinders. To comply with the ISPs is time-consuming, or complying with the ISPs is costly (Chen et al., 2018). Employees may decide not to comply with ISP if they feel that security activities are obstacles to accomplishing the set objectives of their work (Chen et al., 2018)

The perceived self-efficacy to compliance is the level of confidence in one's ability to undertake the recommended preventive behaviour. For example, an employee might perceive (internally reason) (Chen et al., 2018),

"I have the necessary skills or knowledge to comply with the information security policies of my organization";

"I can comply with the information security policies of my organization by myself"; or,

"It is easy to comply with the information security policies of my organization".

Menard, Bott, and Crossler (2017) have found that response efficacy and self-efficacy positively influence the employees' intent to adapt the way they behave.

In summary, what motivates employees to ISP emanates from what the employees perceive as a threat of complying with information security policies and avoiding the negative consequences of non-compliance or complying with security activities. The employee motivation is based on how employees feel vulnerable to the security threat from happening; how the employee perceives the recommended response addresses the threat at hand; or employees may not comply if they think that complying leads to work impediments and is time-consuming. Lastly, the employees may comply with ISPs when they believe it is straightforward to comply.

Therefore, the organisation's goal is for employees to be motivated in complying with regulations for information security and standards to safeguard the organisation's information assets. The following section will discuss information regulation compliance and clarify how non-compliance to security policies by employees contributes to security risks and threats.

2.5. Information Security Regulations Compliance

The foundation for regulating information security compliance in an organisation is applying information security standards (ISM), complying with information security laws and regulations, and adhering to organisational best practices for information security policies. When information security audits are performed regularly, the organisation ensures that its systems comply with standards and guidelines as stipulated in the security policy. Sanctions are imposed for non-compliance with these standards because failing to adhere to security policy is often the cause of poor security in the organisation (Nel, 2017). Compliance with information security regulations can be monitored and evaluated by an independent team or

the organisation itself, often both (Pfleeger et al., 2016). The organisation should monitor data protection law compliance by establishing best practices monitored by an information security oversight committee (Singh et al., 2016). Best practices based on international standards, such as the ISO/IEC 17799, apply to many organisational settings, including the government sector (Saint-Germain, 2017). Raikkonen (2017) states that the ISO 17799/BS 7799 information security standard serves as a guiding principle on the security domains such as security policy, access control, systems development and maintenance and business continuity management.

The following section discusses why an information security audit is an essential part of information security compliance.

2.6. Information security audit

An information security audit checks the system controls for quality, assesses whether employees comply with security procedures, and makes recommendations of any changes that will improve overall information security. The security audit is conducted annually and is certified according to set standards (Raikkonen, 2017). The information security audit should answer the following key questions (Raikkonen, 2017; Singh et al., 2016):

- Is there a committee overseeing information security?;
- What is the impact of the human factor?;
- Has information system risk planning been conducted?;
- Are internal audits being done?;
- Are there any external (third-party) audits required?; and,
- What monitoring is in place for compliance with organisational (departmental) rules and guidelines?

The Auditor-General of South Africa[1] performs information security audits annually within the provincial departments. The security audit is a crucial element for compliance because it checks whether employees comply with security procedures, and the committee makes recommendations for any information security improvements. The security audits assess the organisation's main information assets: hardware, software, and data. So, information security

[1] Within the government sector, the Auditor-General of South Africa is accountable to the National Assembly in terms of section 181(5) of the Constitution and section 3(d) of the Public Audit Act (PAA) No.25 of 2004, and has to report on its activities and performance of its functions in terms of section 10 of the PAA.

audits check whether any vulnerabilities can result in an attack on information-related assets. The following subsection discusses information security asset management.

2.7. Asset Management

A computer-based information system has three critical assets: hardware, software, and data (Joshi & Singh, 2017). Each asset is subject to various vulnerabilities that information security management must consider when planning for information security (Pfleeger et al., 2016). Figure 3. shows the three assets, together with the vulnerabilities (interruption, interception, modification, and fabrication) to each asset (Pfleeger et al., 2016).

- *Interruption* is when an asset of the system becomes unusable, unavailable or lost.
- *Interception* is when an unauthorised party gains access to an asset.
- If the unauthorised user tampers with an asset, that is called a *modification*.
- If the user not authorised to use the asset produces counterfeit objects on the system, that is called *fabrication*.

The best way for proper asset management is the identification of all these assets, identifying associated risks, and putting controls in place to avoid the risks from happening (Nel, 2017).

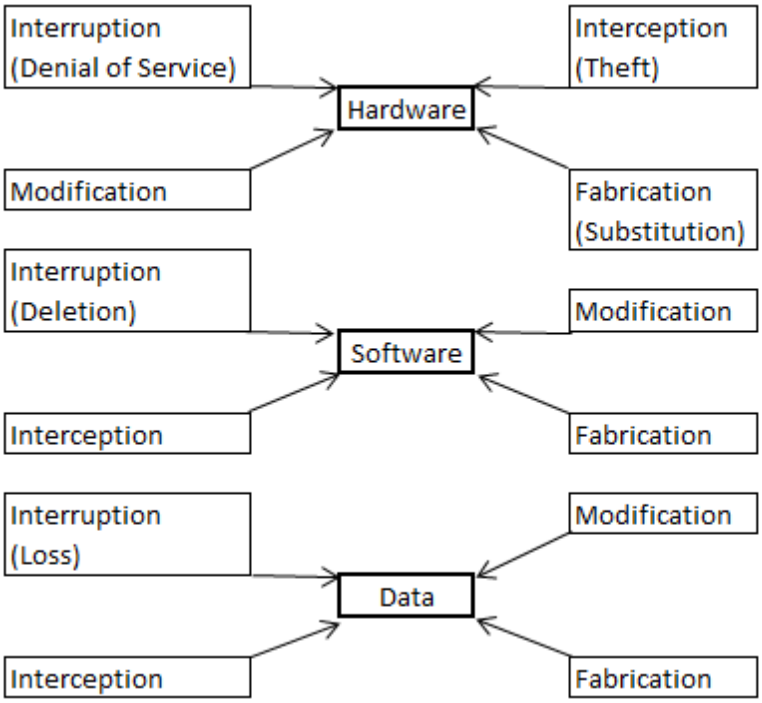


Figure 3: Possible Vulnerabilities of Assets (Pfleeger et al., 2016)

Singh et al. (2016) mentioned among the critical factors of asset management are that the organisation should have an asset register for every information asset (hardware, data and software). Additionally, all organisation business units should record critical information assets and classify information assets according to confidentiality, accountability, or usage. Also required is adequate protection (physical and virtual) of information assets by the organisation. Moreover, there should be a user access control policy specifying users access rights data access rights (Singh et al., 2016).

From the government department perspective, the department has to identify the risk related to each information asset, institute controls for user access to data, maintain an assets register, and classify these assets in terms of confidentiality, accountability or usage. Lastly, implement a software licencing policy that prohibits unauthorised software usage by employees because they can install software with unknown security threats. Without such proper management of assets, employees may intentionally or unintentionally present a severe threat to the confidentiality, integrity and availability of information. When the organisation's information assets are attacked, then those attacks are classified as information incidents. The following section discusses information security incident management.

2.8. Incident Management

Unpleasant events are categorised as incidents when the following features are noticed: they are concentrating on information assets, or if chances of succeeding are high, or they could threaten the confidentiality, integrity, or availability of information resources (Pfleeger et al., 2016). In a security incident, a document called the incident response plan will be used to determine how to deal with the incident (Whitman & Mattord, 2018). An incident can be a single event, a series of events, or an ongoing problem. The procedures described should define what constitutes an incident, identify the responsible party in case of an incident, and describe the action to be taken (Pfleeger et al., 2016).

Singh et al. (2016) mentioned essential information security incident management factors, such as a record of disaster recovery and business continuity plan. After that, processes defining what has to be done should be documented by the organisation when an incident happens. Those processes are then followed by an explanation of disciplinary procedures against

employees who violate information security policies. After that, the disaster recovery and business continuity plan are discussed and communicated to all employees. The sharing of the disaster recovery and continuity plans is the organisation's backup and recovery process to maintain the integrity and availability of necessary information processing and communication services to survive a disaster that may result in the loss of systems and premises.

Additionally, the organisation's historical records/data and information misuse/intrusion attempts/data theft checks should be continuously maintained. Finally, information security measures have to be reviewed regularly - at least once a year (Singh et al., 2016). The actions and processes performed for asset management and those performed during incidence management indicate that these two security management issues are related.

This subsection established that if the attacks on information assets happen, that is called an information incident. The government departments have to manage the incident as per information security management (ISM). The ISM specifies that the department should have an incident response plan for managing incidents. This incident response plan should identify the incidence, the responsible entities, and the action. The significant incident related to this study was that the organisation should take disciplinary action against employees if they have been found to have violated information security rules, and disaster recovery and business continuity plans have to be discussed and communicated to employees.

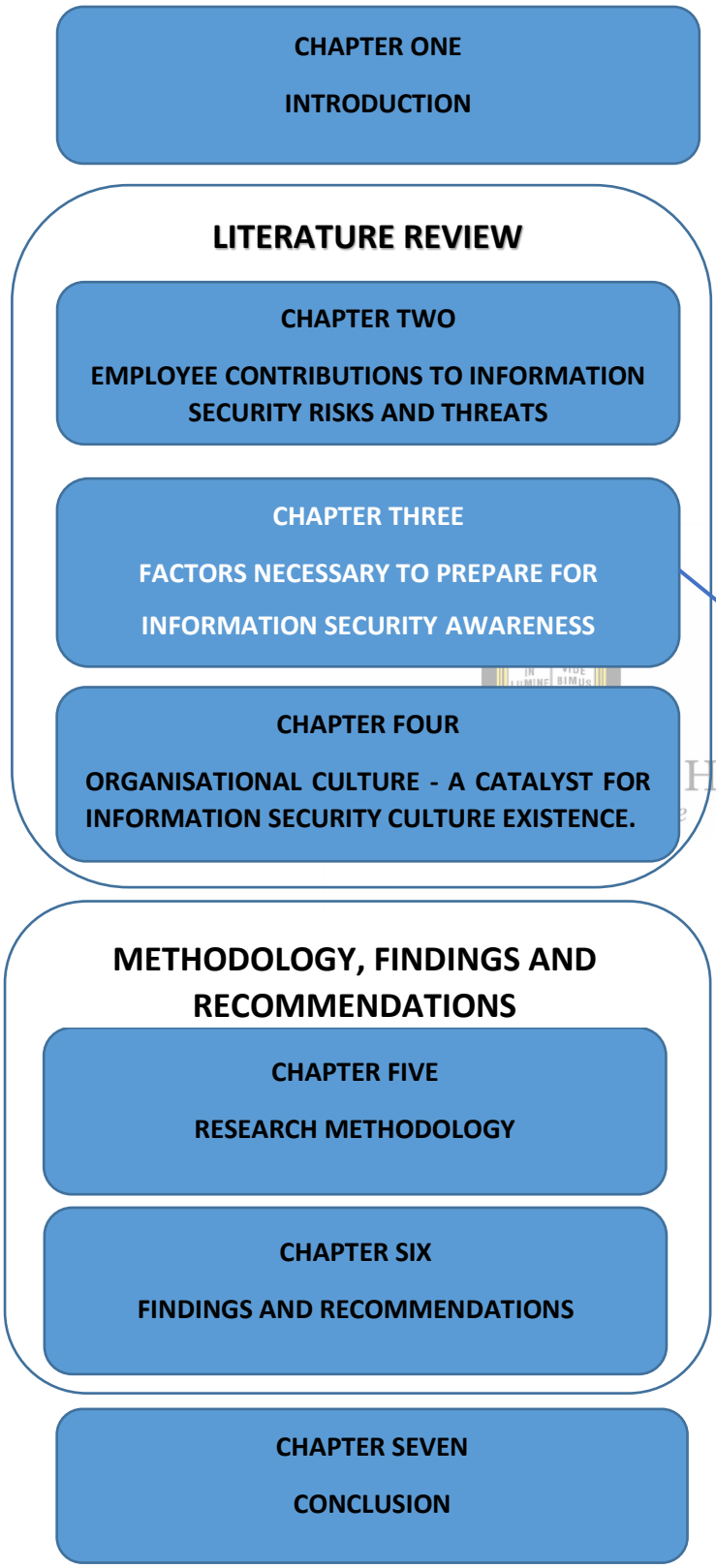
2.9. Conclusion

In this chapter, the research question of how employees contribute to the information security risks and threats has been addressed. Different authors have revealed that complying with information security policy minimises security threats because it clarifies how employees behave. In a provincial government, the departments should have information security policies and ensure that their employees comply with the contents of the policies. The chapter discussed the dynamics of information security risks and threats caused by employees and how best to mitigate those risks and threats. The significance of information security policy as a part of information security compliance was evident throughout the chapter. Then an investigation was made on what motivates employees to comply with information security policy, premised on the Protection Motivation Theory. It was also important to mention the information security regulations and standards that inform the information security policy. Also key was the

discussion on the information security audits, how information assets and incidents are managed.

The chapter discussion made it evident that for employees to comply with information security policies, they need to be aware that the policy exists. Because awareness is vital for the early warning and detection of security risks, the next chapter will review critical factors influencing information awareness programs within the context of this study, i.e. government employees.

CHAPTER THREE: FACTORS NECESSARY TO PREPARE FOR INFORMATION SECURITY AWARENESS



3.1 Introduction

3.2. The nature of Information Security Awareness (ISA)

3.3. The structure of ISA training programme

3.3.1. Steps in the preparation of security training and awareness

3.4. ISA programme in practice: Developed Countries

3.5. ISA programme in practice: Developing Countries

3.6. Challenges of security training and awareness programmes in developed countries

3.7. Information Security Awareness as a catalyst for information Security Culture

3.8. Conclusion

3.1. Introduction

Employee information security awareness positively affects information security compliance in an organisation (Alkabani, Deng, & Kam, 2018). Without employee information security awareness, the organisation can have security breaches irrespective of putting technical and physical security measures in place (Wahyudiwan, Sucahyo, & Gandhi, 2017). Aldawood and Skinner (2019) assert that information security awareness is the only known defence for attacks (e.g. from social engineering). Without employee awareness, the organisation is vulnerable to threats, which place the organisation's information assets at risk. To mitigate the human risk, an organisation should change employees' behaviour, and to change the way employees behave, an organisation requires a mature awareness program (SANS Security Awareness Report, 2019). For a security training and awareness program to be a success, it should be conducted on an ongoing basis, and not just a yearly activity, but should strive to maintain security awareness every day (Stefaniuk, 2020).

The chapter investigates the literature on the factors necessary to prepare an information security awareness program by considering its application in private organisations and government departments in the South African context. The discussion in the chapter focuses on the following areas: the nature of information security awareness, the structure of an information security awareness (ISA) training program, an investigation into awareness activities in government (public sector) settings in developed and developing countries, challenges to ISA rollout, and finally, how ISA fosters an ISC.

3.2. The nature of information security awareness

Employee ISA of information security policies (ISPs) and security threats is critical for effective information security management (Angraini, Alias, & Okfalisa, 2019). Information security awareness is conducted to increase employees' understanding of a security risk to information and control measures thereof and policies to follow (Da Veiga & Martins, 2017). Employees need to understand why compliance is essential, and for that reason, organisations need to improve employees' awareness to build an ISC (Chen et al., 2017; Lohrmann, 2018). An organisation should have an ISA programme to mitigate information security non-compliance because ISA programmes do increase employees understanding and knowledge of security policies (Kweon, Lee, Chai, & Yoo, 2021). Therefore, it follows that employees must be aware of the security risks and threats they face in their daily activities, know how to deal

with them and understand the costs of security breaches (Hamid & Dali, 2020). For example, Jaeger (2018) highlighted how important it is to have an information security awareness program and how having the program influences the employees' perception about the benefits of compliance and the sanctions of non-compliance (*cf*. section 2.4).

Security awareness positively affects employees' compliance with ISPs (Haeussinger & Kranz, 2018). Employee ISA is critical to reducing security risks associated with the manner employees behave towards information security (Bauer & Bernroider, 2018). McCormac et al. (2017) support this statement and assert that when employees gain awareness of the consequences of complying with security policies, organisations can identify strengths and weaknesses and use this information to further their training and awareness programs to improve the information security awareness in the organisation.

Tsohou, Karyda, Kokolakis et al. (2018) further suggest that government employees must be aware of security threats and risks, ensure security compliance towards security policies, and be responsible for the costs and consequences of violating ISPs. Hence there is a need to plan for and prepare an ISA programme for implementation. When implementing ISA programmes, government departments have to consider the challenges and critical success factors from the point of view of (1) the employees as an individual and (2) of the organisation as a whole (Tsohou et al., 2018).

When focusing on ISA factors, some factors influence the employee behaviour (being factors at an individual level) meant for compliance with information policies. These factors rely on employees' motivation to comply (Moody, Siponen, & Pahnila, 2018; McCormac et al., 2017). The awareness factors at the organisational level, for example, organisational culture, assist in providing a guide when designing awareness programmes (Tsohou et al., 2018). European Union Agency for Network and Information Security (2017) undertook a study on ISA factors at an organisational level when focusing on organisational culture. Tsohou et al. (2018) found that some awareness changes should be made at an executive level, impacting information security strategy, power relations, and how duties are allocated. Tsohou et al. (2018) assert that these organisational factors are in addition to the individual factors (employees' attitudes and work behaviour towards security) to make a substantial change in awareness of security breaches.

3.3. The structure of ISA training programmes

The NIST Special Publication 800-16 (2008) asserts that an ISA programme is the means of transportation that an organisation can utilise to convey security requirements throughout the organisation. Therefore, an effective ISA and training program is a suitable platform wherein appropriate security behaviour towards information assets is explained. The program talks about compliance with ISPs. Information security awareness has to precede any sanctions imposed on employees due to non-compliance with ISPs. Employees need information on what is expected regarding information security compliance and exposure to training that includes information security awareness expectations. The structure of an ISA programme requires the organisation to identify the employees' behaviour to be reinforced or discouraged because it provides a clear focus concerning ISA training (McCormac et al., 2017; Hamid & Dali, 2020).

Khando, Gao, Islam, and Salman (2021) proposed that ISA significantly affects employees' confidence in complying with security policies with regards to the benefit of compliance and the cost of non-compliance. Hamid and Dali (2020) discovered that employees' insight on the advantages of information security also understands ISA, which leads to improved compliance with ISPs.

The ideal approach for an ISA and training programme would be to teach employees about information security in general and the organisation's security policy to ensure that employees have the same understanding of the same information security guidelines (Dhakal, 2018). An information security program aims not to educate users about doing their work parse but rather to educate employees about performing the jobs safely and securely (Gilbert, 2017).

The structure of an ISA programme will best be explained by showing the difference between information security awareness, information security training and information security education. *Information security awareness* programs prepare for training by influencing the attitudes of the employees of an organisation towards understanding the importance of information security and the consequences of failing to comply with information security policies which are information security risks and threats (NIST Special Publication 800-16, 2018). *Information security training* is intended to equip the employees with the skills that assist them in doing their work effectively (NIST Special Publication 800-16, 2018). On the

other hand, *information security education* is aimed at ICT security officials and concentrates on strengthening the skills needed to do complex security activities (NIST Special Publication 800-16, 2018).

According to Wilson and Hash (2003), learning is a continuous process as it begins with awareness, builds to training, and then develops into education. This continuum is shown in Figure 4 below.

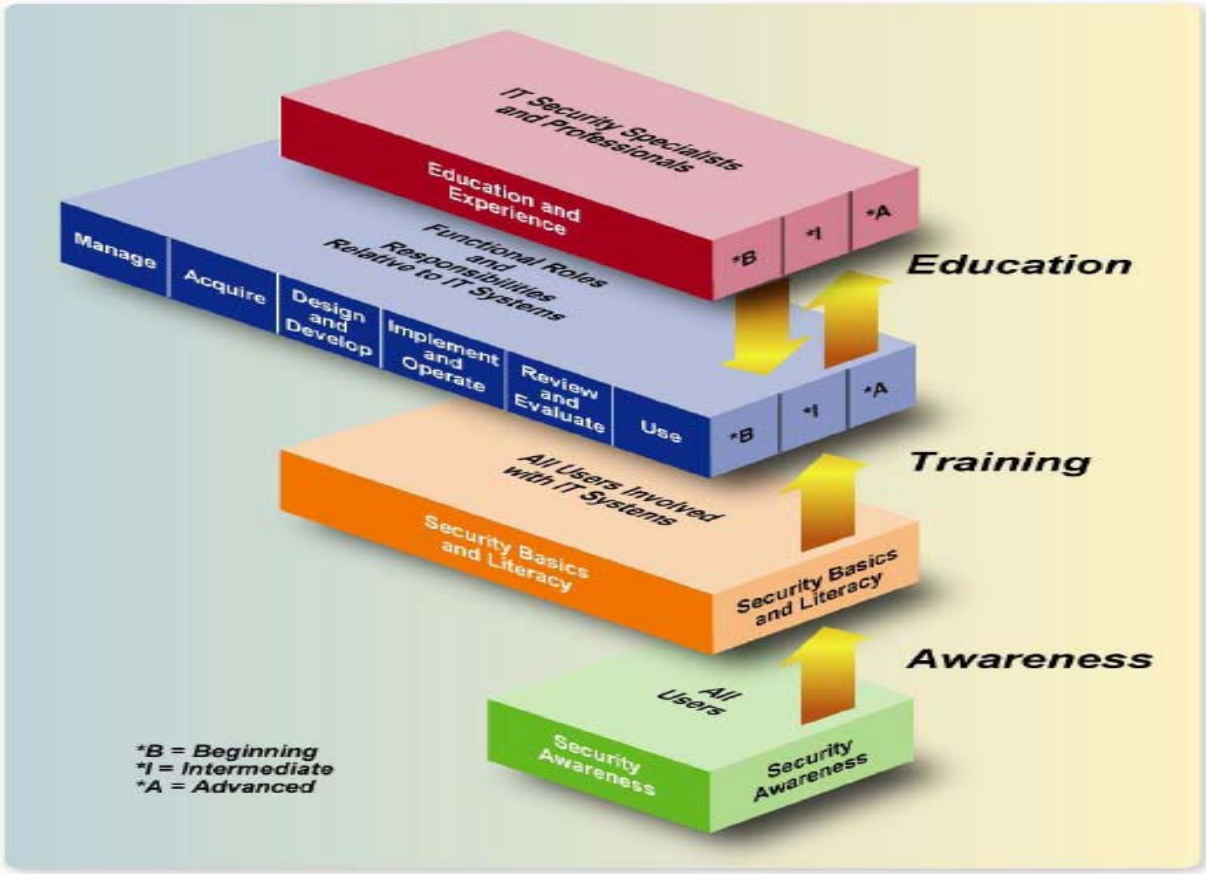


Figure 4: The Learning Continuum (Wilson & Hash, 2003)

The three levels of the learning continuum are explained as follows:

Awareness: As the learner is only the recipient of the information and does not actively participate (NIST Special Publication 800-16, 2018), the aim of the ISA programme is to sensitise and encourage trainees to be security-aware and be reminded of essential security procedures (NIST Special Publication 800-16, 2018). The most effective delivery methods for this learning continuum are posters and flyers.

Training: This learning continuum provides abilities, skills and abilities which are customised to a specific employee based on the role he or she plays within the organisation. (NIST Special Publication 800-16, 2018). Training can either be catered for the general users or advanced users, or users with specialised skills.

Education: The Education level of the learning continuum integrates all of the security skills and competencies of the various functional specialities into a standard body of knowledge. Most organisations opt not to include security education as part of their awareness and training programs as part of employee career development. Nieles, Dempsey and Pillitteri (2017) have a comparative framework for these three levels of SETA, which is illustrated by Table 2. below:

Table 2: The NIST 800-12 Comparative Framework (Nieles, Dempsey & Pillitteri, 2017)

	Awareness	**Training**	**Education**
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Objective:	Recognition	Skill	Understanding
Teaching Method:	Media - Video - Newsletters - Posters, etc.	Practical Instruction - Lecture - Case study workshop - Hands-on practice	Theoretical Instruction - Discussion seminar - Background reading
Test Measure:	True/False Multiple Choice (identify learning)	Problem Solving (apply learning)	Essay (interpret learning)
Impact Timeframe	Short-term	Intermediate	Long-term
Attribute:	"What"	"How"	"Why"

The focus of this study will be on the awareness and training aspects of the continuum. The starting point of an information security awareness programme is to develop awareness, and this will then be extended into training and, eventually, education by reinforcing the lessons learned (Nieles, Dempsey & Pillitteri, 2017). However, material for training should consist of all security-related issues that the participants need to be trained in so that they may conduct their daily tasks according to the direction given during the training. The goal of information security training is to deliver a clear, correct and comprehensive message in a manner that is easily understood by all employees (Dhakal, 2018). The message should focus on *why* the employees have to protect the information and *how* to protect the information.

Information protection is concerned with three attributes of information security: confidentiality, integrity, and availability, which are critical considerations in any training programme (Whitman & Mattord, 2018). The training and awareness programme has to be aligned with the mission of the organisation to achieve the business goals (Breithaupt & Merkow, 2014). The organisation's mission is one of the espoused values explained in the Organisational Culture Theory (Schein, 2004) (*cf.* section 1.6.1.1). Espoused values involve *how* the organisation communicates its strategies, objectives, or public statements of identity (Schein, 2004). After communicating the information security strategy, the organisation begins with employee security awareness and training. The following section discusses the steps necessary to prepare the security training and awareness programme.

3.3.1. Steps in the preparation of security training and awareness programme

Wilson and Hash (2003) stipulate guiding steps (Figure 5) to build and maintain information security training and awareness programmes. These guidelines are Design Awareness and Training Program; Develop Awareness and Training material; Implement Program and Post Implementation. This study will use the NIST 800-50 as a basis for conceptualising a framework for an ISA and training programme for the Eastern Cape Provincial Government Departments.

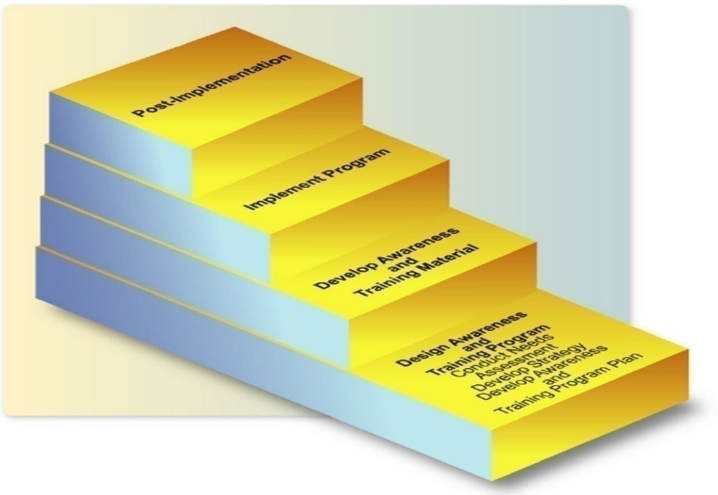


Figure 5: Phases in Preparing an effective IS training and awareness program (Wilson & Hash, 2003)

In the next section, the guiding steps to prepare security training and awareness programme will be explored.

3.3.1.1: Design Awareness and Training Program

The first step is preparing the information security training and awareness program. When designing the security training and awareness program, the most crucial aspect is the department's mission (Wilson & Hash, 2003). Wilson and Hash (2003) state that the organisation's mission is integral to any training and awareness programme. It shows how the business needs fit into the organisational ISC. Therefore, the employees who need to undergo training should feel that the programme's content is relevant to the topics of information security for the organisation and not just meaningless items to them (Wilson & Hash, 2003). If employees have confidence in the relevance of the programme content to the security topics, the self-efficacy on the security awareness topics increase (Wilson & Hash, 2003).

We previously learnt that the Protection Motivation Theory explains that perceived self-efficacy concerns the level of confidence in the employees' ability to understand the content taught, which changes their behaviour towards information security policy compliance (Wu, Stanton, Galbraith, & Cole, 2018). Therefore, information security compliance leads to a reduction of information security risks and threats (Bauer, Beroider, & Chudzikowski, 2017). The design step involves identifying the organisation's needs, target audience, the training and awareness plan outline, setting up the priorities and benchmarks, the training and awareness funding, risk management and business contingency plan (Wilson & Hash, 2003).

As stated in the problem statement (*cf.* section 1.2), ICT audit findings highlight areas of needed improvement in the case of government administration. Wilson and Hash (2003) state that information security audits also have to be studied to get the auditors' recommendations and respond. Consulting the employees to get what they expect from the training and awareness program is also recommended (Wilson & Hash, 2003). Getting employees expectations of training needs will further facilitate the preparation of security training topics.

Suppose an organisation previously conducted information security awareness and training. In that case, the organisation needs to review which topics were covered, how the employees performed on the training, and whether the training and awareness program was completed (Arash & Zarina, 2017). Changes in technology are also very relevant in the review of the

program, so is the level of security threats and risks (Arash & Zarina, 2017). What is also vital is that the organisation needs to identify the security awareness and training tools according to employees' preferences; that will effectively make employees understand the security training and awareness program (Arash & Zarina, 2017).

The organisation should select the right employees for the training based on their needs. The organisation, therefore, has to find out what challenges the target audience is experiencing, and these must find expression in the security training and awareness program (Arash & Zarina, 2017). Additionally, the organisation's executive management needs to support the information security training and awareness programme and decide on this budget (Wilson & Hash, 2003).

3.3.1.2: Develop the security training and awareness program

The organisation should consider whether it will be a *training* whose target audience requires knowledge and education to make the participant learn and apply the skill or *awareness,* emphasising reinforcing the specific behaviour of employees (Nieles, Depmpsey, & Pillitteri, 2017). The emphasis should be on the information that the trainees can implement into their daily tasks (Wilson & Hash, 2003). The awareness material must be engaging with recent or current issues so that the participants may not feel that the material is not customised to their needs; otherwise, participants will participate for the sake of complying with the requirement to attend training (Nieleset al., 2017).

The awareness material needs to focus on a particular security issue, such as sound information security practices and ensuring that employees know their universally shared IT-security responsibilities (Dhakal, 2018). Awareness material can be in the form of websites, blogs, or other forms of popular media that will be appropriate to the intended audience (Wilson & Hash, 2003).

To assess employees' awareness of information security compliance, the organisation can evaluate employees' opinions about the effectiveness of training programs implemented to ensure information security compliance (Alkabani, Deng, & Kam, 2018; Hamid & Dali, 2020). The reason is that positive employees' views on the effectiveness of the training programs indicate that the security training programs were well-structured and well-presented (Alkabani, Deng, & Kam, 2018). Wilson and Hash (2003) state that the list of topics is not finite and

mainly depends on organisational needs. Some examples of these topics are included in Table 3. below.

Table 3: Examples of information security topics (adapted from Wilson & Hash, 2003)

Remote work access protocols	Protection from viruses, phishing, and scams	Information Security Policy
Data backup and storage practices	Social engineering practices	Incident response actions
BYOD security requirements	Password usage and management	Software license restriction issues
Inventory and property transfer	Approved website access	Individual accountability
Securing work devices and information assets	Encryption practices to secure files in-transit	Access control issues

Therefore, within the context of this study, the Eastern Cape provincial government would need to identify the relevant information security training and awareness topics for inclusion in their specific awareness program before implementation thereof.

3.3.1.3: Implement Program

Once the organisation has conducted the needs assessment, designed the training and awareness strategy, and developed the training and awareness material, the next step is implementing the training and awareness program (Wilson & Hash, 2003). Wilson and Hash (2003) state that before implementing the security program, the explanation of benefits to the organisation should be clearly articulated to ensure that the program gets the full support of the management and employees. Informing employees about the advantages of getting their help explains the organisation's effectiveness in persuading employees to change their behaviour as suggested by the Protection Motivation Theory. Moreover, the training and awareness budget must be deliberated upon whether the ICT unit will fund the program or the executive management will budget for it. Hence it is very critical that there is buy-in from the management for the training and awareness program because the management is the final decision-maker to accept and implement the training and awareness program (Dhakal, 2018). Most importantly, the employees' positive participation, interest and complete support matter most because it is only employees who change and not the organisation and therefore, and how employees behave has an impact on the organisation (Dhakal, 2018).

The implementation stage is when suitable training and awareness delivery methods are decided upon (Dhakal, 2018). The decision is whether to create the delivery methods or get freely available online content. The awareness material (Table 4.) should be easily accessible to the employee.

Table 4: Training and Awareness Delivery Methods (Dhakal, 2018)

Delivering awareness methods:	Delivering training methods:
Pictures and posters	Instructor based training
Mouse pad	Computer based training
Screensavers	Scenario based training
Coffee cups	Online forum and interaction
Pens	Group discussion
videos	Focus group
Cartoons	Seminar
Newspaper	Monthly meeting
Security magazines	Conference
Crossword puzzles such as Sudoku	Case study
Calenders	Distance learning and elearning
Security news on Television and radio	Self study (education is training in progress)
Video games	

The recommended way to conduct the security training and awareness programme is to apply more than one delivery method for a successful security training and awareness programme. Dhakal (2018) states that developing a training program sets the tone for the delivery method to be used, whether it is an in-house or outsourced training programme. Training methods are either instructor–based or web-based, or group discussions. Funding has to allow the execution of these methods as some are costly to buy, for example, animated videos.

3.3.1.4: Post-Implementation

Post-implementation continuous monitoring and improvements need to be made to the security training and awareness programme to keep the content current with new threats to the organisation (Ma'ruf & Rochman, 2019; Caballero, 2017). Monitoring whether the training and awareness program was effective is essential for the ongoing improvement of the program. Once training is monitored, it is easy to track and outline key issues that need to be addressed (Caballero, 2017). The ongoing monitoring should undertake feedback and evaluation, focusing on the goals outlined earlier on for the program (Bada & Sasse, 2019).

The section has discussed the four steps in the preparation of the security training and awareness programme. However, we also need to understand the security awareness

programmes rollout done by both the developed and the developing countries to get lessons learnt and find out the success areas and what can be benchmarked from these countries. The following two sections explore the security awareness programmes within the government context.

3.4. ISA programme in practice: Developed Countries

It is essential to mention some examples of awareness programmes developed internationally for the government context.

In Denmark, the local government implemented ISA to conduct competency assessments specifically for information security (ENISA, 2017). ENISA (2017) discovered that teachers and school staff lacked knowledge and available documents on IT security. The government of Denmark then conducted a feasibility study on e-learning applications and prepared information material to pilot the awareness program. The lesson learned was that it was essential to identify a specific audience to target for the ISA programme to realise effective planning and implementation of the security program. Also, it was critical to have an interactive message to promote security awareness adequately. Lastly, the Denmark government prepared an evaluation report for the executive management. An evaluation report is critical for understanding whether the security awareness was effective (ENISA, 2017).

In Finland, the City of Oulu created the Oulu 400 project. Some 400 wireless local networks (WLAN) access points were set up in the city's busiest areas so that citizens could be allowed to search the Internet for free. The aim was to ensure that there is the utilisation of wireless services. The project had a security module with advice for citizens on improving information security in their everyday life (ENISA, 2017).

The Australian government also conducted an ISA study to research whether ISA amongst government employees caused behavioural change towards information assets (Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2016). Parsons et al. (2016) also suggested how selecting training programs can improve compliance with security policies by tailoring content for the trainees' needs.

The French government conducted ISA programs utilising a multiplier (in adult education centres, service providers, unions, banks or community centres) as a delivery method of

information security awareness to the target group and larger public (Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2016). France recommended using quizzes as time-saving, to test employees knowledge, utilising channels such as brochures, leaflets and fact sheets to attract employees' attention. The government of France used the following channels for information security awareness: television before the news, websites of ministries involved and web portals of private partners.

Observing the developed countries as discussed above, most of them made use of multipliers The multipliers can be the option to be used in the framework prepared for security awareness in this study. Secondly, during preparation for the awareness programs, the developed countries identify a specific audience so that there is effective implementation of security awareness and training. They also prepare an evaluation report after the awareness and training program to assess the impact of the training (Wilson & Hash, 2003).

3.5. ISA programme in practice: Developing Countries

As the previous section showed how the developed countries implemented the ISA programme, it is also essential to discuss how governments in developing countries have prepared the ISA programme. Wahyudiwan, Sucahyo, and Gandhi (2017) explain that due to high-security incidents in government systems in Indonesia, there was a need to put in place information security controls to mitigate information security risks. A study was then conducted to ascertain whether the government employees of a specified department had adequate information security awareness levels. Employees' knowledge, attitude, and behaviour were assessed to establish a viable and feasible ISA programme. Parsons, McCormac, and Butavicius (2016) stated that ISA measurement often uses focus areas. Wahyudiwan et al. (2017) researched the implementation of seven focus areas (Table 5.) initially developed by Parsons, McCormac, Pattinson, Butavicius, and Jerram (2016). The Australian government applied these. The focus areas explain information security policy items that relate to an employee and often lack employee compliance. In addition to the focus areas, some sub-areas indicate common examples of areas where unintentional human errors occur.

Table 5: Information security Focus Areas (Parsons et al., 2016)

Focus Area	Sub-Areas
Password management	Locking workstations Password sharing Choosing a good password
Email use	Forwarding emails Opening attachments IT department level of responsibility
Internet use	Installing unauthorized software Accessing dubious websites Inappropriate use of the internet
Social networking sites (SNS) use	Amount of work time spent on SNS Consequences of SNS Posting about work on SNS
Incident reporting	Reporting suspicious individuals Reporting bad behaviour by colleagues Reporting all security incidents
Mobile computing	Physically securing personal electronic devices Sending sensitive information via mobile networks Checking work email via free network
Information handling	Disposing of sensitive documents Inserting USB devices Leaving sensitive material unsecured

Wahyudiwan, Sucahyo, and Gandhi (2017) revealed that although ISA levels within government employees were relatively good, employees still needed to improve in certain areas such as password management, email use, social networking sites and mobile computing. The lessons learnt from the government of Indonesia (Wahyudiwan, Sucahyo, & Gandhi, 2017) are that:

- the government needed to develop more detailed information security policies that are related to the requirements of a focus area;
- develop ISA programme and monitor employee compliance and promote employee awareness of their security responsibilities;
- conduct annual employee ISA measurement due to newly appointed employees each year, new trends in information technology and measure the latest conformity to information security by employees.

The Malaysian government discovered that building a sound ISA training program relies heavily on the chosen delivery method, design, and training content (Newton, Anslow, & Drechsler, 2019; Ghazvini & Shukur, 2017). Malaysia developed the Training Method Selection Framework as a recommended guideline to choose a training delivery method for information security (Alshaikh, Maynard, Ahmad, & Chang, 2018; Ghazvini & Shukur, 2017). The study utilised the involvement of decision-makers to provide their insights to develop the framework. The Training Method Selection Framework is illustrated in Figure 6. below.

For the Malaysian study(Alshaikh, Maynard, Ahmad, & Chang, 2018; Ghazvini & Shukur, 2017), details of common human errors were collected using a questionnaire. The training content was developed from the incorrect answers from the human errors collected. The framework aimed to outline the essential characteristics of an effective delivery method. The delivery method is composed of training success factors and training needs. The framework could promote employees' motivation and participation in training activities. Additionally, the security content of the framework can be utilised to prepare security training content for employees. The training content can improve and strengthen the information security understanding of employees, especially on ISPS.

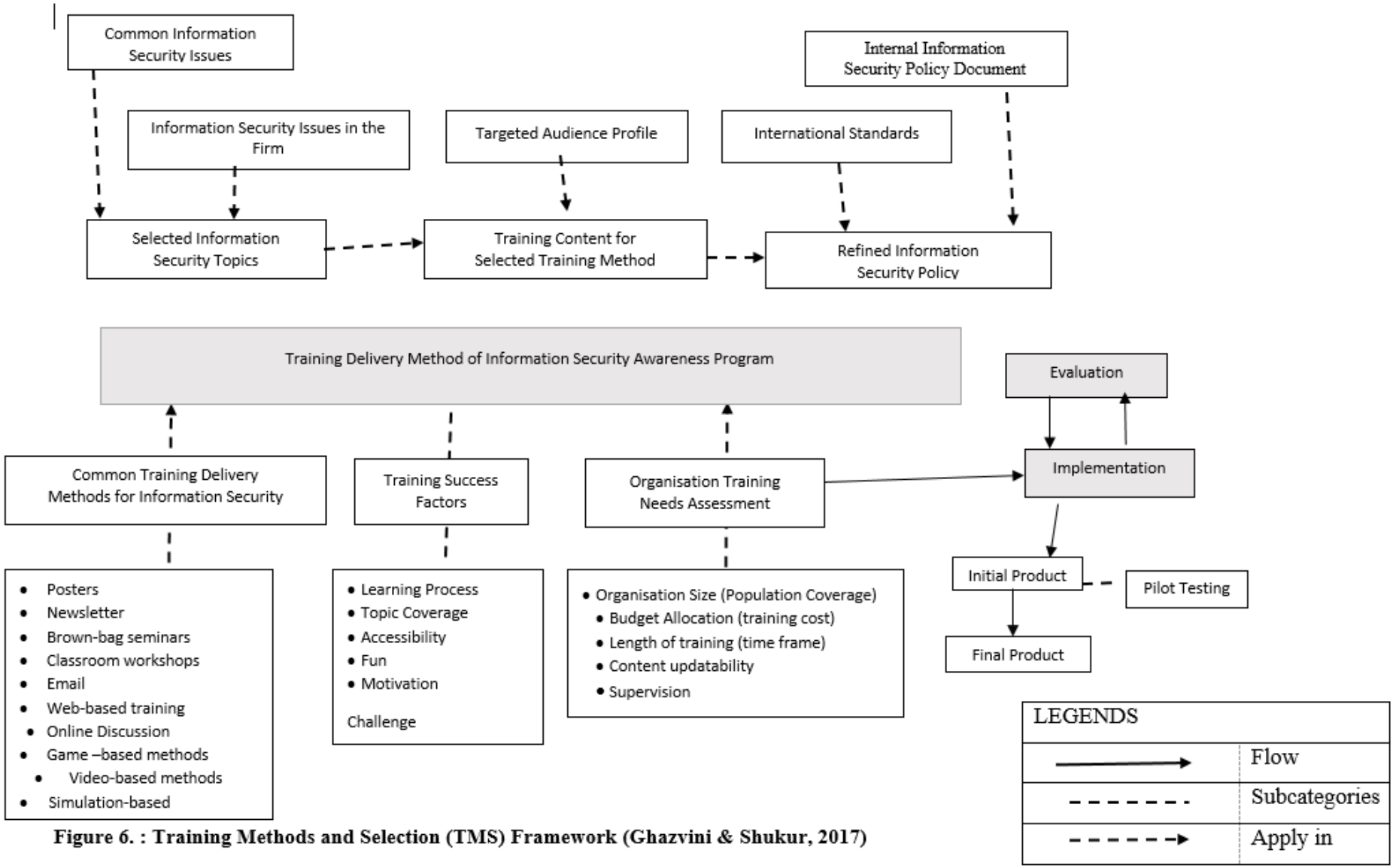


Figure 6. : Training Methods and Selection (TMS) Framework (Ghazvini & Shukur, 2017)

Bada and Sasse (2019) warn that there may be unexpected challenges when implementing the training and awareness program. The following section discusses those challenges that may arise in the implementation of security training and awareness programme.

3.6. Challenges of security training and awareness programmes in developed countries

During the implementation step of a training and awareness programme, an organisation may encounter challenges. For example, the organisation may enrol all participants in the same program irrespective of previous experience or security background as a cost-saving measure (Dhakal, 2018; Ndiege & Okello, 2018). But the focus and speciality of awareness training need to be tailored to each employee's function and role within an organisation (Labuschagne, 2017). Therefore, not all security awareness training is equal. The training selected for an organisation should suit its specific needs, its business environment and its level of security maturity (Labuschagne, 2017). An organisation might be challenged by not clearly defining funds for the training and awareness programme (Dhakal, 2018; Wilson & Hash, 2003). Additionally, an organisation might lack resources and materials (Dhakal, 2018; Bemis, 2017).

Another challenge is that employees know the answer to awareness questions when asked; however, employees' security activities are not the same in practice (Bada & Sasse, 2019). Therefore, the security awareness programmes can fail regardless of the previous research findings that indicate that information security awareness can lead to improved information security behaviour and ISP compliance (Bauer, Bernroider, & Chudzikowski, 2017). It is essential to understand why security awareness programmes can fail to change the behaviour of employees after they have attended the awareness and training sessions.

Bada and Sasse (2019) investigated why security awareness campaigns fail and found that how the employee responds to the recommendations from the security awareness programme is dependent on the sanctions for non-compliance as stated in the security training and awareness programme, and the employee's self-efficacy toward those recommendations (Bada and Sasse, 2019). Self-efficacy is the level of confidence in one's ability to undertake the recommended preventive behaviour, which is one of the tenets of the Protection Motivation Theory (Clubb &

Hinkle, 2018). Bada and Sasse (2019) recommend that if security awareness is to succeed, the expected behaviour change, as suggested by the programme, should be simple and easily understandable, emphasising the advantages of implementing the security awareness programme.

An employee's security compliance motivation is based on whether they feel vulnerable to a security threat, how they address the recommended response threat or believe that compliance will lead to work impediments and is time-consuming (Bauer et al., 2017). Lastly, the employees may comply with information security when they feel it is easy and straightforward (Bada & Sasse, 2019). Bemis (2017, p2) asserts that the key challenge with the need for the simplicity of security policies is that most security policies are "developed to sound like legal prescripts and the main aim being to keep the organisation out of trouble more than to provide information or influence employee's behavioural change".

Therefore, it is advisable to simplify ISPs for employees to ensure they are understood and accessible to employees so that they can be applied by employees (Bemis, 2017). Simplifying security policies should be manifested again in designing security awareness and training messages because the main aim is to change employees' security behaviour (Kritzinger, Bada, & Nurse, 2017).

To change the security behaviour of employees, an organisation should empower its employees with not just information about risks and expected security behaviour, but employees should understand and apply the advice (self-efficacy). Secondly, employees must be motivated and willing to do so (perceived response efficacy). Lastly, employees must have changed their attitudes and intentions *(Perceived Response Cost)* as suggested by the Protection Motivation Theory.

For effective implementation of ISA and training programme on employees, the programme should not impose excessive fear (sanctions) on simple, consistent rules of behaviour that are easily followed. It is important that the ISA and training programme be easily understood and be not technical and be easy to (Labuschagne, 2017).

Amjad, Naeem, and Zaffar (2016) suggest that adult trainees need to be actively engaged and the material immediately valuable and relevant to their day to day life to be effective. Amjad et al. (2016) raise the following points that will impact the effective implementation of the security awareness programme:

- *Continuous training and feedback* are essential to support employee behaviour after noticing they are willing to change their behaviour following an implemented security and awareness programme.
- *Lack of a robust organisational security strategy*. Information security is a strategic risk management issue for organizations of all types and sizes. However, there is often no detailed and solid security strategy where the organisation can draw clarity and consistency. Bemis (2017) warns that unless organisations consider security awareness and training as part of a more holistic defence-in-depth security layer of security, it will never have the legitimacy required for organizational adoption.
- *Executive-level visibility, support, and enforcement* are about setting the 'tone from the top' and leading by example (Bada & Sasse, 2019; Dhakal, 2018). If employees don't see security being taken seriously by upper management, they cannot be expected to be serious about security awareness matters (Bemis, 2017).
- *Information has value,* and anyone encountering that information should have an understanding of its importance, reasons for its importance and reasons for its protection is essential. An organisation needs to aim to instil behaviours aligned to the organisation's security goals, which is done at a cultural level. Moreover, the training programme should be based on their own organisation's culture, policies, procedures and perceived threats (Amjad, Naeem, & Zaffar, 2016).

Additionally, there should be an understanding that information security concerns cut across the organisations and not just an IT challenge but a business challenge.; similarly, ISA and training are meant to be conducted for both IT staff, and all employees can access the internet and computer (Labuschagne, 2017; Da Veiga & Martins, 2017; Mahfuth, Yussof, Baker, & Ali, 2017). Information security awareness and training can assist in developing an effective security culture in an organisation accompanied by a rise in employees' avoidance of information security risks and threats (Da Veiga, 2016).

Therefore, ISA and training programmes can assist in teaching an ISC in which everyone in the organisation assumes responsibility for information security. The next session discusses how information security training and an awareness programme can enable an organisation to build an ISC.

3.7. Information Security Awareness as a catalyst for information security culture

Employees should have the necessary information security education training and awareness, and motivation to comply with ISPs (Chen, Ramamurthy & Wen, 2015). If there is insufficient support for information security training and awareness, employees could be reluctant to demonstrate an expected change of behaviour or always find excuses for not complying (Chen et al., 2015). Hence information security awareness (ISA) programs are suggested and introduced into organisations to improve compliance with ISPs (Bauer & Bernroider, 2018; Belanger, Collignon, Enget, & Negangard, 2017; Pattabiraman, Srinivasan, Swaminathan, & Gupta, 2018).

Most security training and awareness programs aim to instil a strong sense of security among employees. Instilling a sense of security ensures that information security becomes a natural, integral part of their day-to-day information related jobs (Whitman & Mattord, 2016). Detailed information security training and awareness programmes try to change the behaviour of employees concerning information security and motivate employees about security when they perform their daily jobs. Nevertheless, the fundamental influences to change behaviour are shared security attitudes, values, and beliefs. Previous research has focused on building an ISC in an organisation (Mousavi & Kumar, 2019). Security culture assists organisations in achieving their security end goals – to promote security behaviour and employee security values (Chen et al., 2017).

Schein (2004) asserted that organisational culture could be shown at three different levels—artefacts, espoused values and the last, taken-for-granted assumptions. At the level of the **artefact,** one can observe organisational culture by objects, for example, employee behaviour or organisation's buildings. Employee's behaviour can not be understood by just organisational culture as an organisational culture just a surface level (Schein, 2004). Following artefacts are the **espoused values level** where organisational culture shows itself in an organisation's vision, mission, norms, and other higher-level thoughts expressed in the organization's public documents and in the mechanisms to implement and enforce those vision, mission, norms, and beliefs (Arbanas, Spremic, & Hrustek, 2021).

Security education, training, and awareness programs are well-known means of building employees' awareness of the organisational vision, mission, norms, and thoughts in a format of the organisation's public documents (Arbanas et al., 2021). Therefore, security training and

awareness programs intend to move organisational culture from the surface level to the espoused values level with a deeper level of employee thoughts and perceptions (Arbanas et al., 2021). The highest level of culture means that the shared, **taken-for-granted assumptions** are created and deeply set up among employees (Schein, 2004). The organisational culture at this level shares values and beliefs which are deeply entrenched in employees' daily job-related behaviours. To achieve the highest level of culture, organisations prepare and implement comprehensive security programs to create shared, taken-for-granted assumptions (Schein, 2004). Based on Schein's organizational culture theory (Schein, 2004), Chen et al. (2017) contend that, similarly, ISC has three levels, as shown in Figure 7.

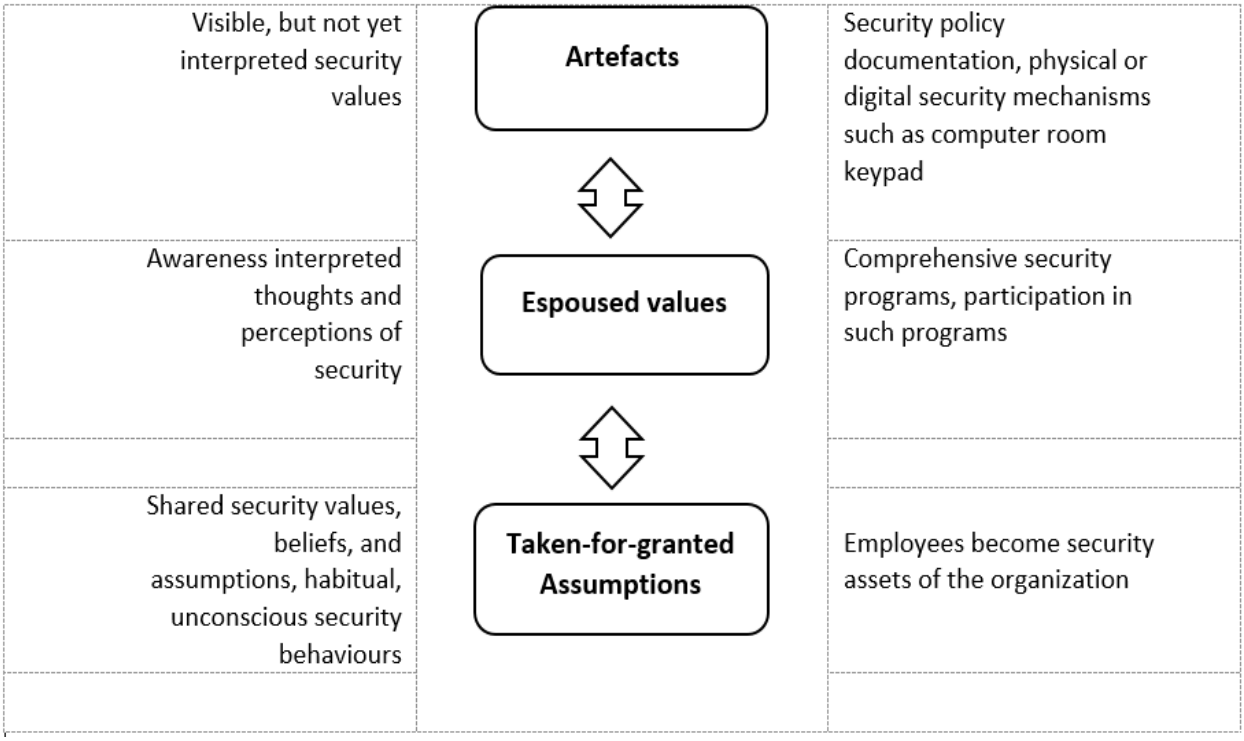


Figure 7: Information security culture framework (Chen et al., 2015)

Artefacts are all security procedures, which are visible or observable, such as computer-room locks, video surveillance systems, and authentication processes. *Espoused values* level are all ISPs, ISA and training programs. ISPs articulate information security-related vision, mission, norms, and other higher-level thoughts of the organisation and serve as a basis for creating shared values and assumptions in information security. Information security training and awareness programs implement the control and ensure employees' awareness of values and beliefs find expression through the security policies. Lastly, the *taken-for-granted level* assumptions are the

shared security thoughts and perceptions that are related to security values and beliefs, which become strong forces to guide how employees behave (Nasir, Arshar, Ab Hamid, & Fahmy, 2019)

Chen et al. (2015) discovered that security training and awareness programs strongly influence the security culture in organisations. Therefore, a well-prepared and implemented security training and awareness program can change the way employees perceive, feel, and apply their beliefs about information security and change them to protect information security assets even at the cost of extra effort and workload. In addition, security training and awareness programs can instil an organizational security culture in which everyone assumes responsibility for information security.

3.8. Conclusion

The chapter sought to explore the main factors that influence information security awareness amongst employees. Reviewed literature has confirmed that government employees should be aware of the security threats and risks mentioned in the information security policies. Furthermore, government employees also need to be aware of the consequences of security breaches from non-conformance to these policies, which necessitates preparing security training and awareness programmes for government employees.

To embark on security training and awareness programmes, it is necessary to determine the level of security literacy of employees, and after the training to establish if the security knowledge has been acquired. The chapter discussion highlighted that the content in information security training and awareness programmes should be aligned with the organisation's mission and culture specifics. The content of the programme should include those security topics that are relevant to employees' jobs. It was also emphasised that when employees have been trained on suitable topics, this increases employees' self-efficacy and confidence levels, which are instrumental in changing employees' behaviour towards information security policies.

The success of an information security awareness campaign relies on the programme's benefits is explained to the management of the departments for the necessary buy-in and allocation of funds to the programme. Choosing the appropriate awareness delivery method that's suits the department to be trained was highlighted as a key factor.

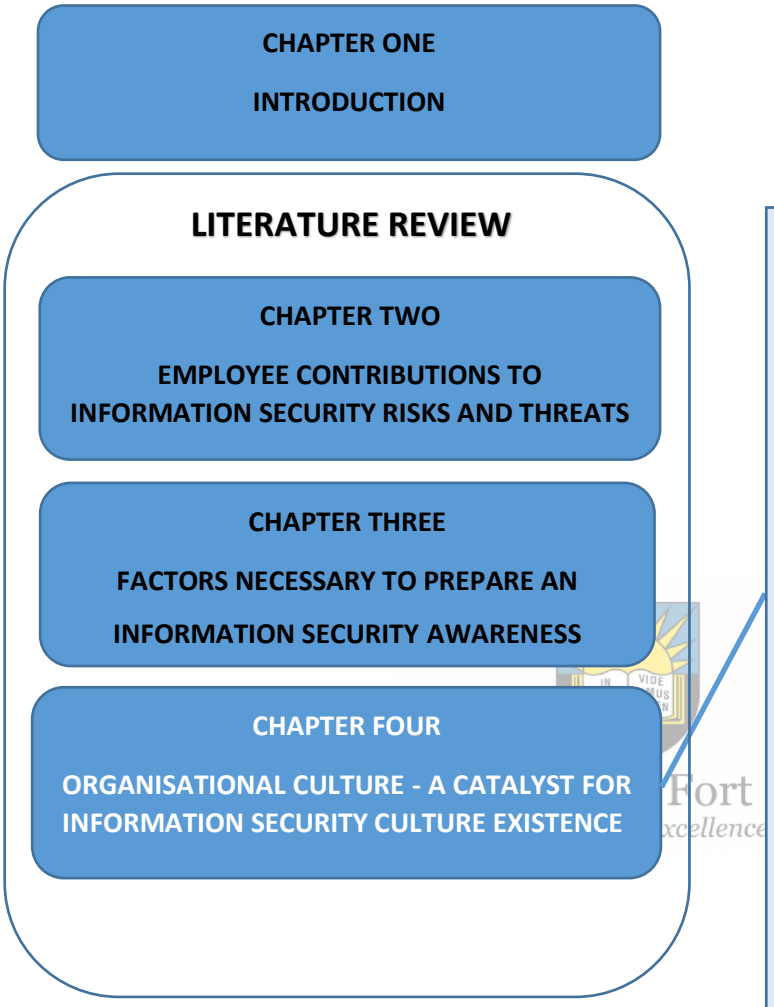
The lessons learned from the implementation of information security programmes in developed and developing countries have been explored. In addition, the challenges encountered by

developing countries will ensure that these challenges become lessons learnt to prepare the Eastern Cape provincial government information security awareness programme.

Finally, the chapter discussed how information security awareness programmes could be the vehicle to instil an ISC within government departments.

The next chapter discusses the requirements to foster an ISC in the provincial government.

CHAPTER FOUR: ORGANISATIONAL CULTURE - A CATALYST FOR INFORMATION SECURITY CULTURE EXISTENCE



4.1. Introduction

4.2. Differences between organisational culture and information security culture

4.2.1. Organisational culture

4.2.2. Information security culture

4.3. Assessing the current information security culture

4.3.1. Defining Information Security Culture Assessment (ISCA)

4.3.2. Utilising ISCA results to improve security culture

4.3.3.Assessing the existing security culture

4.4. Determining employee attitudes and perceptions towards information security culture

4.5. Key aspects of information security culture

4.5.1. The role of Top management

4.5.2. Compliance

4.5.3. Security Awareness, training, and education

4.6. Conclusion

4.1. Introduction

Information security culture (ISC) is defined as how employees behave when handling information, whether it is organisational systems and cyberspace, which is expressed as behaviour in an organisational context that affects information protection (Astakhova, Botha, & Herselman, 2020). The aim is to instil a culture in which information assets, including employees, are valued and protected, thereby obtaining social and economic benefits for the organisation (Da Veiga et al., 2020; Doherty & Tajuddin, 2018). An improved ISC helps organisations reduce security risks and threats to information assets (Nel & Drevin, 2019). By instilling an ISC, an organisation can motivate employees to protect information assets against numerous security threats (Al Hogail A. , 2015).

Therefore, an organisation's ISC has to be established to signify the way employees behave concerning the managements' information security goals, ensuring that goals are not miscommunicated (Shouran, 2019; Thomson & Van Niekerk, 2011). Organisational culture reduces miscommunication by creating shared beliefs and values as there is no need to communicate things about which shared values exist. Shared beliefs and values help employees to interpret the vision, strategies, policies developed by management in the same way (Shouran, 2019; Thomson & Van Niekerk, 2011). Additionally, the organisation's security education, training, and awareness (SETA) programs can be a powerful strategy to enhance employees' compliance and assist in securing the organisation's information assets. The SETA programs can also assist in forming up an organisational culture that appreciates the employees' behaviour that complies with security policies, thereby mitigating security risks and threats (Chen, Wu, Chen, & Teng, 2018).

Nel and Drevin (2019) assume that an ISC is part of organisational culture because information security is one of the organisation's functions. The ISC is often perceived as a subculture of organisational culture that mainly focuses on ensuring that information security is the natural aspect of the daily lives of employees (Nel & Drevin, 2019; Da Veiga & Martins, 2017).

This chapter will discuss the differences between organisational culture and ISC. After that, the importance of assessing ISC is briefly considered, which can be looked at from various angles. Following that will be a discussion about employee attitudes towards ISC. Finally, key identified aspects of ISC, namely the role of top management; compliance; security awareness, training, and education, are presented to establish an ISC.

4.2. Differences between organisational culture and Information security culture

4.2.1. Organisational culture

Organisations are expected to show that they have acted with due diligence about information security as expected by the policy; hence security involves everyone in the organisation, not just IT officials (Vijayan, 2018). This is because security is not just about ensuring that there are firewalls installed or password and awareness training conducted to employees, but it is also about instilling a culture that makes employees perceive information security seriously and correctly (Okere, Van Niekerk, & Carroll, 2017). Organisational culture is there to shape and direct the behaviour and attitudes of employees, and as such, there is a need to understand the organisational culture when learning about ISC (Connolly & Lang, 2018). Baker (1980, cited by Connolly, Lang, Gathegi, & Tygar, 2017) stressed that the value of organisational culture is instrumental in leading an organisation either to success or failure since organisational culture affects employees' behaviour.

Developing organisational culture can be made a source of reference when developing ISC. However, for an organisational culture to develop, the top management of that organisation should first develop its vision and strategy (Kassem, Angappa, & Helo, 2018). The vision and strategy are usually shown and incorporated into the policies and procedures of that organisation. So will be the behaviour of its employee. Over time, organisational culture will also develop, which includes the vision and strategy, and the experiences shared by employees when implementing them (Nel & Drevin, 2019). When an organisation is known to have bureaucracy as its culture (such as the government setting), where all employees are forced to play by the rules, everyone complies with the information security policies more strictly than in informal and individualistic cultures (Nel & Drevin, 2019). Hence it is critical to note that altering an organisational culture would effectively focus on changing unchanging employees' behaviour and processes (Nel & Drevin, 2019).

The organisational culture must show a good attitude towards information security for the whole organisation (Ashenden, 2018). It is also key that the activities performed in an organisation be consistent with the practices of a good ISC (Amankwa, Loock, & Kritzinger, 2018; Palega &

Knapinsski, 2019). Hence the management of the organisation must establish a security culture within the organisational culture (Karlsson, Denk, & Åström, 2018).

To understand how an ISC evolves, an understanding of how an organisational culture develops is crucial. Organisational culture is created where an organisation's top management or leadership draws a vision and strategy generally stated in the organisation's policies and procedures (Da Veiga & Martins, 2017). Da Veiga and Martins (2017) further note that employees' behaviour will be guided by the vision, strategy, and policies. As time goes on, organisational culture will manifest, including the vision and strategy and the employees' experiences of executing these strategies. An ISC concept in an organisation evolves in the same manner as the organisational culture. Organisational culture is defined as,

> "*A pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration to be taught to new members as the correct way to perceive, think, and feel concerning those problem*s" (Schein, 1992, pp. 12).

Schein's definition fundamentally focuses on two issues. The first one is that the shared basic assumptions of the group should be defined, and the second one is that every employee who forms part of the organisation should be taught about these assumptions. It is a big task to define and develop these shared assumptions that have to be accepted by the employees and the organisation's management. Determining the shared expected assumptions can be done by the organisation's management through developing policies (Da Veiga and Martins, 2017).

Culture includes norms about how things are done and facilitates how the group perceives and thinks (Schein, 2004). The Theory of Organisational Culture (Schein, 2004) understands culture as having three hierarchical levels: Artefacts and creations, Espoused Values, Norms and Knowledge, and Basic Underlying Assumptions and Beliefs. This theory is vital to understanding organisational culture.

The organisational culture depends on the basic assumptions and beliefs that shape the employees' behaviour regarding their thoughts and feelings (Von Solms & Von Solms, 2004). Therefore, the organisation's culture demonstrates procedures, processes, or rules that ultimately influence employees' behaviour, resulting in artefacts.

In addition, education, training and awareness are vital in fostering a culture in the organisation (Von Solms & Von Solms, 2004). Therefore the management of the organisation should shape the behaviour of the employees to that which benefits the organisation by dictating how employees should behave, and organisational culture is critical in ensuring whether the organisation succeeds or fails because organisational culture directly shapes the behaviour of employees (Connolly & Lang, 2018). Management can convey collective values, norms, and knowledge by outlining specific policies and procedures that reflect the required underlying assumptions. Schein's theory asserts that the vision of the management results in organisational culture (Von Solms & Von Solms, 2004).

It is essential to understand the organisational culture to define and understand the ISC (Ruighaver, Maynard, & Chang, 2007). For an organisation to have successful information security, security must be firmly embedded within the organisational culture (Da Veiga & Martins, 2015). Hence ISC is always regarded as a sub-culture of organisational culture (Conolly, Lang, Gathegi, & Tygar, 2017). Therefore, security culture cannot be assessed in isolation but within the organisation's overall culture. The following section discusses the ISC.

4.2.2. Information security culture

Risk mitigation caused by not adhering to ISPs by employees (the human factor), it is suggested that organisations instil a culture of information security (Okere, Van Niekerk, & Carroll, 2017). The reason is that ISC is a discipline that looks into the employees' beliefs, knowledge, attitudes, and assumptions that serve as a guide for what activities to undertake to safeguard the organisation's information assets. Information security also ensures that employees behave acceptably by looking at information security as one of the activities to be considered daily (Al Hogail & Mirza, 2017)

Fostering an ISC to safeguard information assets by directing an organisation on how to protect information assets and by exercising guidance on the behaviour of employees regarding security is one of the ways that can assist organisations in reducing risks that are caused by humans (Tolah, Furnell, & Papadaki, 2017). The risk of security threats due to a lack of protection of information assets caused by employees is mitigated when an organisation has an ISC (Nel & Drevin, 2019). Since human beings are the weakest link concerning the protection of information assets,

organisations should foster an ISC and have deep insight into the various types of security threats (O'Brien, Islam, Weng, Xiong, & Ma, 2018; Connolly & Lang, 2013).

Information security culture is set to align with the way employees behave in an organisation setting to safeguard information. Employee security behaviour is manifested by complying with information security policies and requirements and knowing how to cautiously and attentively implement such policies, as emphasised through consistent communication, awareness, training, and education programs. After a long time, employees' behaviour becomes part of the way things are done due to employee's assumptions, values and beliefs, their awareness of, and attitudes and perceptions of protecting information assets (Mahfuth, Yussof, Abu Baker, & Ali, 2017; Nel & Drevin, 2019). The ISC is guided by the vision of senior management together with management support according to the ISP and is noticeable in the artefacts of the organisation and behaviour exhibited by employees (Nel & Drevin, 2019).

The most detailed adaptations of Schein's (1992) theory of organisational culture to security culture were done by Da Veiga and Eloff (2010), and van Niekerk and von Solms (2010). Van Niekerk and von Solms (2010) adapted Schein's model for clearly reflecting security culture and added the knowledge tier. Da Veiga and Eloff (2010) concentrate on the relationship between information security, behaviour, and culture, across the individual, group, and organisational levels. ISC is perceived as a sub-culture of the organisational culture that focuses on information security (Chen, Ramamurthy, & Wen, 2015; Tolah et al., 2017).

ISC is influenced by the environments inside and outside the organisation. (Da Veiga & Martins, 2015). The environment inside the organisation comprises elements such as leadership and organisational structure, and the environment outside the organisation is composed of the economic climate to the industry's technology intensity. Da Veiga and Martins (2015), Da Veiga and Eloff (2010), Schlienger and Teufel (2003) are of the view that these environments bring about certain behaviours reflecting the way things are habitually done in a particular organisation. A robust security culture occurs when employees are aware of security risks and threats; and measures to prevent such risks (ECD, 2015). The main aim of a robust culture is the protection of information assets through instilling a working environment that promotes that workers do the right thing.

Organisational culture is instrumental to building an ISC when an organisation adopts and diffuses information security (Chen et al., 2016). According to Chen et al. (2016), ISC follows Schein's definition of organisational culture, and therefore ISC is a procedure of how security things are done. The definition includes creating an environment that teaches ISC and is defined as doing things around information security. Additional to creating an ISC environment is creating an environment that instils and supports shared security attitudes and values in a particular organisation (Chen et al., 2016; Van Niekerk & Von Solms, 2010). ISC is a combination of all explicit and implicit means to assist in shaping the attitudes of employees and behaviours towards information security (Van Niekerk & Von Solms, 2010).

When an organisation has an ISC, its employees naturally demonstrate the expected information security attitude and behaviour in a taken-for-granted manner (Chen et al., 2016). For example, employees can have a strong security attitude towards using strong passwords regardless of the extra effort (Chen et al., 2016). Based on Schein's organizational culture theory and Van Niekerk and Von Solms' security culture framework, ISC also has three levels (Nasir, Arshar, & Ab Hamid, 2017; Chen et al., 2016). These levels are:

Level One: Artefacts

The observable security procedures and processes, for example, video surveillance systems, mechanisms to authenticate employees of the organization, computer room locks security policies, are artifacts (Chen et al., 2016). Artefacts symbolise the outside physical expression of culture (Cotter-Lockard, 2016). These artefacts are observable things that employees can see and the behaviour they can measure in an organisation (Okere et al., 2012). So patterns of behaviour, security handbooks, awareness courses, language, and technology are artefacts. Even though this level of information culture is easy to see and observe, it is not easy to explain without questioning the organisation's employees (Okere et al., 2012).

Level Two: Espoused Values.

Espoused values are related to the assumptions because ISC comprises employees' shared security values, beliefs, and assumptions about information security. Espoused values are comprised of education, training and awareness programs, security policies, and monitoring. These espoused values are put together and determined through the formed perceptions of employees when they interpret artifacts, and perceptions are created after having undergone security education training and awareness programs (Chen et al., 2016). Espoused values are not as obvious to observe as

artifacts; however, these values can influence employees' behaviour. Espoused values justify why employees follow the artifacts. The examples of espoused values are strategies, goals, philosophies, and other documents that describe the organisation's values, principles, and vision (Okere et al., 2012).

Level Three: Shared Tacit Assumptions

Shared tacit assumptions generally develop in organisations that have been successful and can be attributed to the management's values, beliefs, and assumptions in the organization. After instilling these values and beliefs, they become shared values and beliefs. When successfully implemented, the values and beliefs turn out to be shared basic assumptions and beliefs become the central element of the organisation's culture (Schein, 2004).

Security policies outline information security vision, mission, and norms and establish shared values and assumptions in information security in the organisation (Chen et al., 2016). Security education, training and awareness programs, and security monitoring are where control mechanisms are being implemented to ensure that employees are aware of values and beliefs expressed in the security policies (Chen et al., 2016). Shared security perceptions aligned to security values and beliefs of the organisation finally become the taken-for-granted assumptions and ultimately become the forces guiding how employees should behave (Chen et al., 2016).

Information security culture is a subculture of organizational culture. Information security culture is a culture that correctly interprets information security issues and not only in the sense of firewalls, passwords, and awareness training. It should be entrenched into the organisation's culture so that employees understand the security challenges correctly. As a result, Schein's model is used (Schlienger & Teufel, 2003).

The description is not necessarily for information security but is known as a general organizational culture definition hence the enhancement by Van Niekerk & Von Solms (2010). Van Niekerk & Von Solms (2010) describes ISC by adapting Schein's model and adding a fourth level, *information security knowledge* which supports the other three levels (Figure 7).

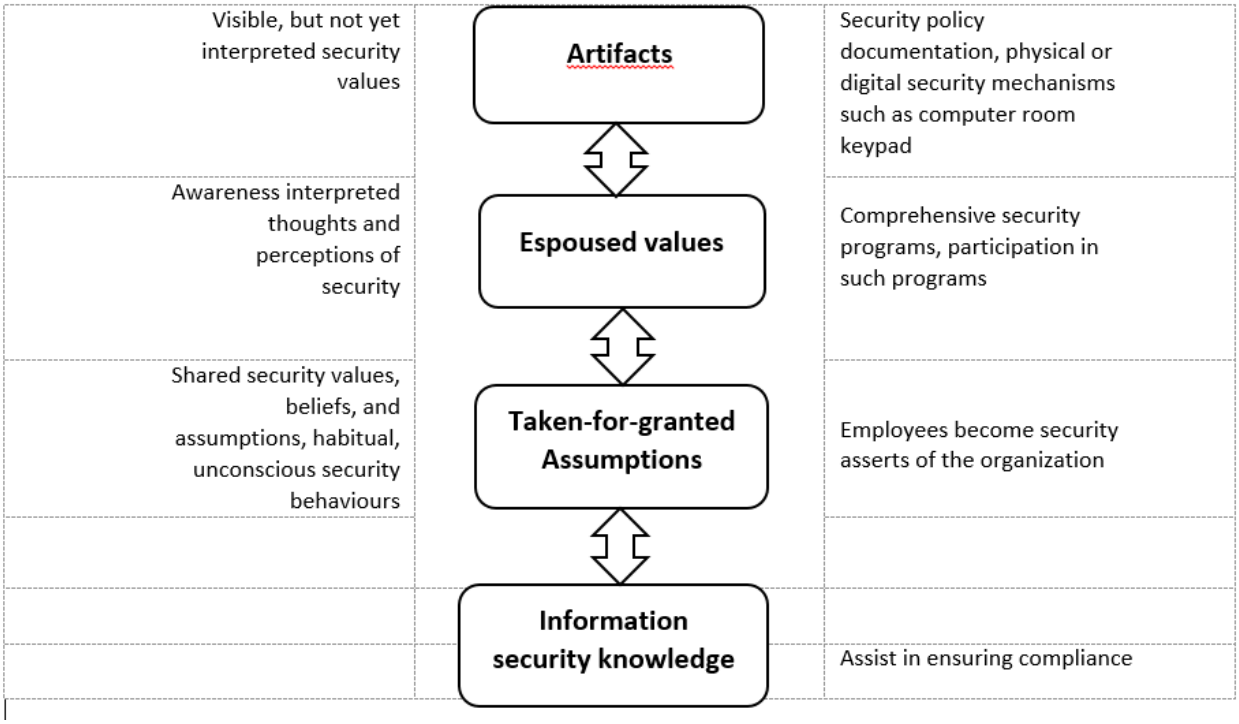


Figure 8: Information Security Culture Framework (Da Veiga & Eloff, 2010)

Information Security Knowledge level supports the other three levels in the following manner:

- *artefacts* (enough information security knowledge to behave securely in their daily activities when interacting with information assets),
- *espoused values* (employees should know the portion to contribute with on the ISP during the ISP development in the organisation guided by what they already know about information security, for example, to ensure that it adequately addresses the security needs of the organization), and
- *shared tacit (taken-for-granted) assumptions* (if an employee's beliefs conflict with an espoused value, for example, not knowing why a specific control is required, the employee might knowingly disregard the security control).

Information security culture can be created where employees have security knowledge and perceptions about information security policy rules and procedures (Whitman & Mattord, 2021). Knowledge could thus help in ensuring compliance. The information security policy serves as a critical basis for directing the ISC and is an essential cornerstone for creating shared values and beliefs (Box & Pottas, 2013). Information security knowledge is necessary if employees behave securely, as it cannot be assumed that the employees possess such security knowledge.

4.3. Assessing the current ISC

The verb "assess" means "to estimate the value or quality of" (Oxford, 1983, 2005). "Assess" in the context of this study refers to pinpointing whether there is an adequate level of an ISC that can offer quality safeguarding of information assets. An adequate level of ISC is described as the level that provides sufficient safeguarding of information assets and reduces the security threats to the information asset's confidentiality, integrity, and availability.

4.3.1. Defining ISC Assessment (ISCA)

An ISC assessment (ISCA) instrument assists in determining whether the ISC level of an organisation enhances the protection of information assets, thus minimising the threat to its confidentiality, integrity, and availability (Nel, 2017). The findings from utilising the instrument help provide a guide to positively shape areas that need to be developed of employee behaviour and attitude (Nel, 2017; Da Veiga & Eloff, 2010). These assessments should determine and report the state of ISC in the organisation (Da Veiga & Eloff, 2010). The employees 'attitudes and perceptions about information security should be established for an organisation to assess the ISC (Da Veiga, 2016). The results from assessing how employees perceive ISC can assist in identifying areas that need to be attended to to improve the ISC to the desired level. The desired level will ensure the protection of information assets (Da Veiga & Martins, 2017). According to Da Veiga et al. (2007) and Da Veiga and Eloff (2010), the ISCA can be administered using a questionnaire.

The purpose of assessing ISC is to assist an organisation in instiling ISC so that employees understand the confidentiality and sensitivity of the information and properly handle the information. Additionally, assessing information security helps identify the key elements (leadership, trust) organisations require to improve the safeguarding of the organisation's information from a human perspective.

4.3.2. Utilising ISCA results to improve security culture

The results arising from assessing information security give a measuring tool that an organisation can utilise to emphasise key areas that an organisation should focus on. Focusing on these areas enables the employees to comply with information security requirements outlined in the information security policy. Da Veiga (2016) states that an ISC can be affected positively by implementing the ISC assessment tool and using what the assessment result recommends. Da

Veiga (2016) indicates that ISA and training contribute significantly to instilling an ISC in organisations.

Assessing information security raises awareness of safeguarding information assets in the organisation, and by so doing, contributes to fostering an ISC (Da Veiga, 2016). Employees who received information security training appeared to have a more positive ISC (shared culture) than those who did not undergo such training. Da Veiga (2016) says that organisations can improve the extent of their ISC by implementing the ISC assessment and its proposed recommendations. Additionally, concentrating on ISA and training positively impacts the ISC and improves the ISC over time. The employee who is not complying with ISPs is guided on how to correct such behaviour due to the excellent effect of ISC. Assessment of information security can help direct and prioritise ISA and training since it emphasises the security topics on which the organisation needs to focus. Moreover, the assessment suggests other means that an organisation can implement to reduce risks related to human behaviour to protect the organisation's information. Da Veiga (2016) further indicates that the assessment of ISC can be enhanced by verifying if the way employees perceive is aligned with the way they behave towards complying with security policies which are usually checked by IT audits and monitoring.

Tolah et al. (2017) suggest a framework that seeks to integrate all essential factors and differentiate between factors that constitute and influence ISC. This can be done by concentrating on human aspects for measuring the level of information security to understand the challenges of information security (Tolah et al., 2017).

4.3.3. Assessing the existing security culture

Assessing the organisational culture's current status is critical when instilling ISC (Da Veiga, 2019, Al Hogail, 2015; Okere, Van Niekerk, & Carroll, 2012). Al Hogail (2015) adds that because of an assessment of the current ISC, the organisation can identify vulnerabilities and threats to information assets and quickly take corrective actions. Okere et al. (2012) focused extensively on assessing tacit assumptions and lacked details on artefacts, espoused values, and information security knowledge. Okere et al. (2012) suggest that organisations should assess ISC through auditing processes as an integrated approach that seeks to assess all the dimensions in the ISC.

To achieve this, an organisation needs to monitor ISC using the ISC assessment instrument to assess the employees' attitude, knowledge, opinions, and how they behave towards information security (Da Veiga & Martins, 2015). The findings from this assessment can be utilised for directing how employees should interact with information assets to mitigate the threats that employees pose to the safeguarding of information assets (Da Veiga & Martins, 2015). The assessment can also help identify the training and awareness requirements that the organisation should conduct to foster a more robust ISC (Da Veiga & Martins, 2015; Nel, 2017).

A strong security culture is critical to reducing security risks and threats caused by humans in an organisation to safeguard the information assets (ENISA, 2017; Al Hogail, 2015). Having a robust security culture leads to the reduction of risk of workers who misbehave, strengthens complying with security policy and regulations, enhances the organization's security standpoint and seeks to reduce security incidents or breaches that are due to the way employees behave (Mahfuth, Yussof, Baker & Ali, 2017; Van Niekerk & Von Solms, 2010; Verizon, 2021).

Flores and Ekstedt (2016) assert that the ISC of an organisation is positively associated with employees' attitudes towards security threats. The following section discusses the importance of determining the attitudes and perceptions of employees towards information security

4.4. Determining employee attitudes and perceptions towards information security culture

Instilling an ISC can reduce the risk caused by how employees interact with the organisation's information assets. Moreover, having a security culture can minimise the threats related to employees who misbehave concerning their interaction with information assets (Verizon, 2021; Van Niekerk & Von Solms, 2010). The lack of information security awareness and attitudes of employees significantly contributes to security incidents and threats. So there is a need to foster an ISC so that the behaviour of employees can be influenced in the organisation (Mahfuth, Yussof, Abu Baker, & Ali, 2017).

The ISC influences the information security behaviour of employees; as a result, the required knowledge guides the behaviour of employees in an organisation (Flores & Ekstedt, 2016). Organisations may use awareness and training to shape employees' attitudes and perceptions towards information security (Da Veiga & Martins, 2015; Ashenden & Sasse, 2013; Ifinedo, 2014). Employees should behave appropriately and have the necessary attitude towards

information security, and that security behaviour can be attained by ensuring that security knowledge is provided to employees (Nasir, Arshah, & Hamid, 2019). This knowledge and behaviour must be aligned to have a successful ISC (Mahfuth et al., 2017).

Parsons et al. (2015) suggest that when an organisation improves its ISC, employees behaviour toward information security assets is influenced positively, leading to improved compliance with security policies. Including compliance activities daily on employees, work practices help employees to understand information security requirements while their behaviours are trained to be aligned with information security policies (Kolkowaska, Karlsson, & Hedstrom, 2017; Tang, Li, & Zhang, 2016)

Tolah et al. (2017) concluded that security culture implies that security issues are considered part of organizational operations. Therefore awareness and understanding of security are fundamental to establishing a successful ISC.

4.5. Key aspects of information security culture

It is assumed that creating a security culture can effectively influence employees' security compliance (Sherif, Furnell, & Clarke, 2016). This section aims to identify factors or aspects that the organisation requires to cultivate a security culture. The aspects being discussed are the role of top management, compliance and awareness, training and education. These aspects will ensure that ISC is adequately fostered in the organisation.

4.5.1. The role of Top management

Nel and Drevin (2019) highlight that one of the effective ways to cultivate and reinforce a culture is to consider "what leaders pay attention to, measure and control". Leaders who express their expectations and entrench them gradually and continually in the organisation's vision, mission, goals, structures, and working procedures foster a culture. Therefore, culture begins with its leaders – management plays a critical part in establishing culture (Martins and Martins, 2016). Likewise, ISC is institutionalised by management via their information security values which cascade down to all levels of employees (Nel & Drevin, 2019).

Their vision is expressed through the ISP (Thomson & Van Niekerk, 2011), which sets the tone for safeguarding information assets. Subsequently, employees will comply ISPs based on what motivates them to comply. The ISC that later develops can either support the safeguarding of

information assets or hamper them. Hence, it is critical to assess the information security that has since developed and ascertain if it aligns with the first information strategy and vision set out by the management (Nel & Drevin, 2019). The management needs to outline the organisation's information security strategy and lead by example (Hu, Dinev, Hart, & Cooke, 2012; Johnson & Goetz, 2007; Knapp, Marshall, Rainer, & Ford, 2006). It is the responsibility of the organization's management to create an environment for learning the values of the organisation for its employees and assist them to be capable of complying with ISPs; so that information security compliance can improve (Chen, Wu, Chen, & Teng, 2018).

Chen et al. (2018) suggest that as much as penalties do matter, however, the focus of the information security management program should be on developing informal sanctions and awareness and training. Thus, to motivate employees to comply with information security policies in an organization, management should focus less on sanctions and more on fostering a compliance culture and, most importantly, availing the resources (e.g. conducting awareness sessions, budgeting for information security) (Masrek, Harun, & Sahid, 2018).

Karyda (2017) also adds that management at all levels, from lowest to highest, has a critical role in shaping organisational culture and bringing about change. Masrek et al. (2018) indicated that management support, among other factors, is essential to instilling an ISC. Management can show commitment by continuously communicating information security policies issues and building a security culture around compliance.

4.5.2. Compliance

Compliance refers to adhering to the information security policies by employees while they perform their jobs (Li, Stafford, Fuller, & Ellis, 2017). Information security compliant behaviour influences the protection of information resources. Consequently, employees should reflect on the consequences of how they behave towards their information security as they interact with the organisation's information assets (Gangire, Da Veiga, & Herselman, 2019; Connoly, Lang, Gathegi, & Tygar, 2016). When employees understand that their security behaviour has an essential consequence of the organisation's goals, they will comply with the organisation's security policies (Gangire et al., 2019).

Soomro, Shah, and Ahmed (2016) assert that employees' knowledge of information security policies positively changes employees' attitudes towards complying with information security

policies. As a result, an effective ISC has compliance as a visible trait (Da Veiga, Astakhova, Botha, & Herselman, 2020; Safa, Von Solms, & Furnell, 2016; Furnell & Clarke, 2015). For example, as part of compliance with information security policy, an organisation may specify that a password should be kept secret and securely at all given times by employees. The password policy, by specifying that, seeks to direct the behaviour to safeguard information assets by controlling who can access the information. The aim is to change the behaviour of employees and to make sure the information assets are protected.

Gangire et al. (2019) note that compliance should not be due to being forced to comply but should be due to individual self-motivation or choice. For example, employees display compliance when

- they choose strong passwords, avoid using the default security password, avoid sharing passwords with other system users (Blythe, Coventry, & Little, 2015);
- back up necessary data regularly and store the backups in a secure location (Ifinedo, 2012); and
- do not disclose sensitive information (Safa, Sookhak, Von Solms, Furnell, & Herawan, 2015).

Employees, therefore, need to be aware and be trained in implementing these security controls. The following section discusses security awareness, training and education.

4.5.3. Security awareness, training, and education

According to Da Veiga and Martins (2015), ISA and training positively influence ISC. Implementing ISA and training aims to make employees understand and be aware of the risk and threats to information assets and the necessary controls that need to be in place. An organisation that conducts ISA and training succeeds in creating an ISC over time (Parsons et al., 2015; Da Veiga, 2013). Organisations should promote information security awareness to investigate the effectiveness of organisational culture on ISC. Therefore management support and employee security awareness are the most crucial elements for ISC (Mahfuth, Yussof, Abu Baker, & Ali, 2017).

4.6. Conclusion

This chapter discussed the role of organisational culture as an enabler for establishing an ISC. The factors that are required to foster ISC were then discussed.

The discussion of the differences between organisational culture and ISC was expanded because a successful establishment of ISC cannot be assessed in isolation but within the organisational culture. This was explained by focusing on how the organisation's management should establish the ISC within the organisational culture to motivate the employee to behave to safeguard the information assets. Later on, the chapter concludes with a discussion of how the assessment of the current ISC can enable the organisation to know the level at which the organisation is protecting security assets to reduce security risks and threats. Additionally, the results of the assessment enable the organisation to identify areas of improvement.

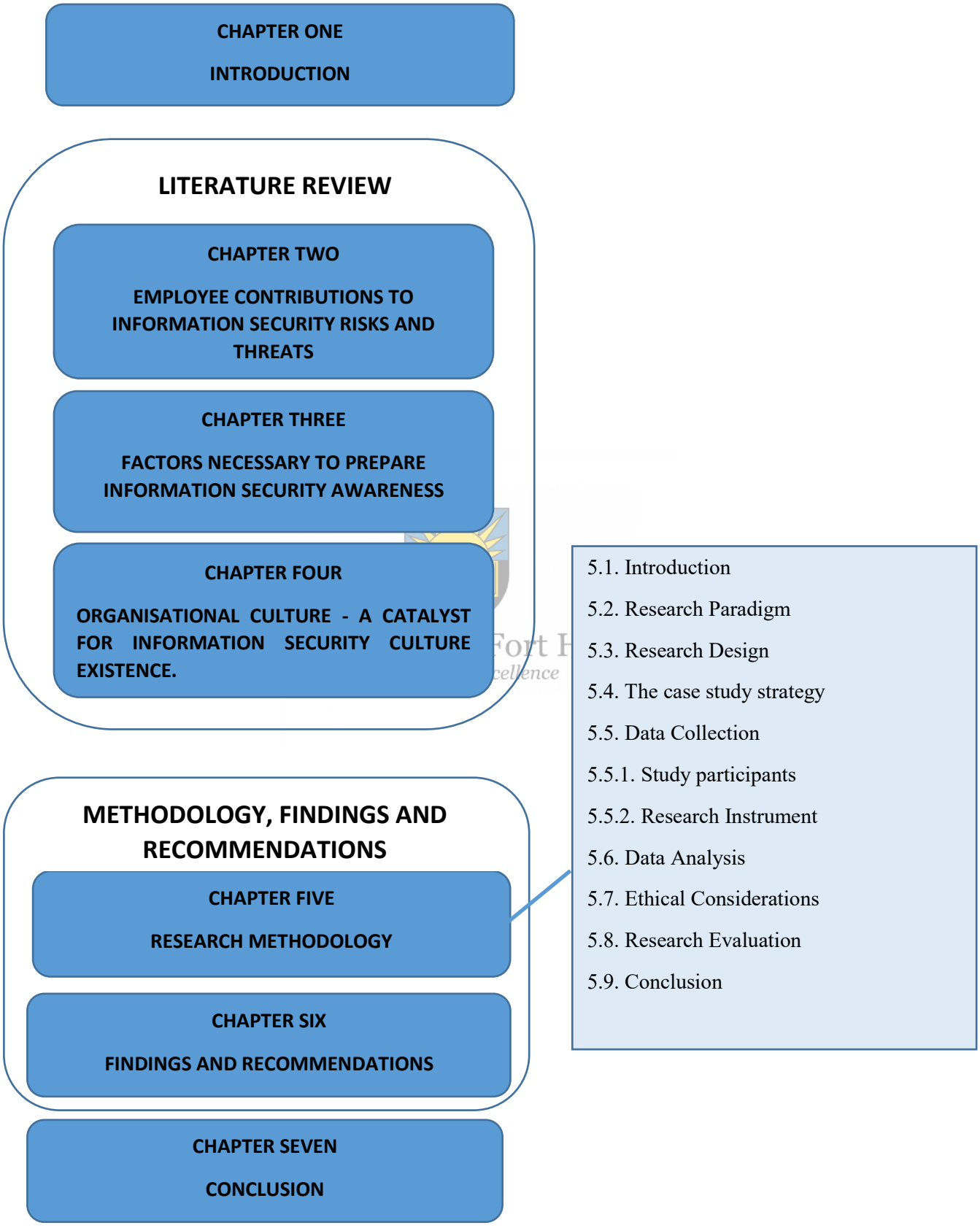
The importance of ISC in influencing the behaviour of employees and motivating employees compliance with security policies was elaborated. Additionally, the role played by the organisation's top management was emphasised as the management's responsibility is to create an environment for employees to learn the organisation's values and, therefore, would be instrumental in assisting employees in complying with information security policies. ISC can, therefore, be cultivated where employees have a good perception and knowledge about security policies. Thus, information security policies play a pivotal role in influencing the ISC and establishing shared values and beliefs.

Additionally, the chapter concludes that awareness, training, and education improve employees' understanding of security risks and threats to information assets and ways to control them.

From a theoretical perspective, this chapter detailed some issues surrounding the tenets of the Organisational Culture Theory such as employees' patterns of behaviour or awareness courses which is the principle of Organisational Culture Theory (*Artifacts*); security strategies, the vision of the organisation, which is the principle of Organisational Culture Theory *(Espoused values)*; Shared security values, habitual and unconscious security behaviours which assist in ensuring compliance which is the principle of organisational theory (*shared tacit assumptions*). The Protection Motivation Theory was implied by considering that when an organisational culture encapsulates ISC, the management may see improvement in employees' perception of understanding security policies. The organisation assumes that employee compliance should not be forced but should be due to individual self-motivation or choice. This is the fundamental principle of perceived self-efficacy, which stresses the level of confidence in one's ability to undertake the recommended preventive behaviour.

The next chapter discusses the research methodology used for collecting the data that must be analysed to inform the development of the **framework to prepare an information security awareness and training programme for a provincial government department in the Eastern Cape**.

CHAPTER FIVE: RESEARCH METHODOLOGY



5.1. Introduction

The research problem is primarily based on the researcher's philosophical assumptions (research paradigm) or the researcher's perception of the world of research and the research methods suitable for the chosen study. Therefore, it is critical to understand these philosophical statements (research paradigm) to investigate and evaluate the research. This chapter will briefly introduce the philosophical research paradigms. After that, the design strategies that underpinned this research project will be discussed. Next, the research paradigms are compared to decide on the appropriate choice for this study. The remaining part of this chapter focuses on the research method and aspects of the research design used in the research project.

5.2. Research Paradigm

A paradigm is a set of beliefs in the mind of a researcher concerning the world and how they participate in that world (Kivunja & Kuyini, 2017). These beliefs are based on the philosophical assumptions related to how one gets knowledge about it (epistemology) and the nature of how we perceive the world (ontology) (Saunders, Lewis, & Thornhill, 2009; Rechberg, 2018).

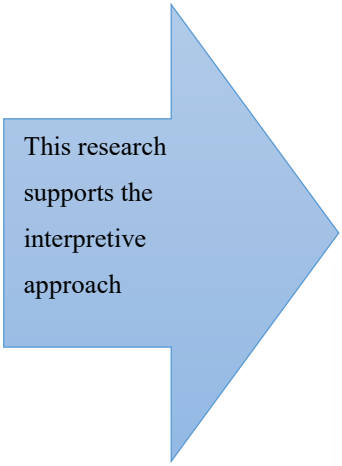
Myers (1997; Hassan, Mingers, & Stahl, 2018) mention three distinctive philosophical assumptions that are used in research and that all research studies are categorised into these philosophical assumptions. They are the positivist, interpretive and critical assumptions. The differences between the three philosophical assumptions are also highlighted in Table 6. below.

Interpretivism focuses on understanding the social part of an information system: social impacts influence the system and its effects on people (Oates, 2006). Interpretive research assumes that knowledge of reality can be acquired via social constructions such as consciousness, tools and other artefacts, and a shared language only (Klein & Myers, 2001).

There are three basic principles of interpretive research (Cooper & Schindler, 2014, p.17):

- The world is created, and the people provide its meaning.
- The study's researcher is not neutral; instead, the researcher participates and is part of the observation.
- Peoples' interest who conduct the research drive the research.

Table 6: Research paradigms (Kivunja & Kuyini, 2017.p30)

Research paradigms	Description
Positivist	▪ Regards reality as factually provided and can be described by measurable properties, independent of the observer and their instruments. ▪ It exists if "there is evidence of proposition, quantifiable measures of variables, hypothesis testing, and the drawing of inferences about the phenomenon from a representative sample to a stated population", p.30. ▪ It is concerned with revealing what is true and describing it empirically.
Interpretive 	▪ Access to reality is only through social concepts, for instance, language, consciousness and shared meanings. ▪ The interpretivist understanding of the world is through the meaning that people give to the world, and when people are no longer part of that world, that meaning stops existing. ▪ It is underpinned by observation and interpretation; therefore, observing collects information of events, and interpreting explains what the information means. ▪ The objective is to provide insight and contextualise the information system. ▪ Emphasises the importance of putting analysis in context. ▪ Unlike positivists, he does not seek to understand dependant and independent variables but is concerned about understanding the human interest.
Critical Social Paradigm	▪ Presumes that reality is historically constituted, produced, and reproduced by people. ▪ The ability to consciously act to change social and economic circumstances is constrained by various social, cultural, and political domination forms. ▪ Socially critical, restrictive and alienating conflicts and contradictions of the status quo are brought to light. ▪ The intention is to openly critique the status quo, focusing mainly on the conflicts and constraints in contemporary society and seeking to find cultural, political and social change that would remove the reasons of alienation and domination.

Based on the information provided in Table 6. the description of positivism and critical social paradigm is not appropriate for this study. The right paradigm for this study is interpretivism.

5.3. Research Design

Myers (1997) argues that as much as there are various classifications of research methods, they are commonly distinguished by whether they are either qualitative or quantitative research methods or mixed methods. In addition, Myers (1997) states that quantitative research methods originated from the natural sciences to research natural experiences. The aim of developing qualitative research methods in the social sciences was to allow researchers to investigate both social and cultural experiences.

Queirós, Faria, and Almeida (2017) argue that the reason to do qualitative research emanates from observing that people communicate their lived experiences in the real world. Queirós et al. (2017) pointed out that people can construct social and cultural concepts by interacting. Qualitative research facilitates the understanding of the social components necessary to develop information awareness in employees. The information awareness programmes rely on successfully communicating it to create or strengthen their messages. Therefore qualitative research helps to realise how effective communication results in effective awareness programs. This assists in reducing information security risks that occur due to poor compliance with information security policy.

5.4. The case study strategy

According to Farquhar (2018), the method of study provides a strategy of inquiry that moves from the underlying philosophical assumptions to research design and data. Strategies of inquiry guide the researcher towards the procedures used in a research design (Creswell, 2014). The researcher has to state the strategy of inquiry because it justifies the study's credibility for future research (Creswell, 2014).

Patton (2018) states that a case study addresses what is required for this research project because it aims to find out the current phenomenon, especially when more clarity needs to be sought to compare the real-life context and the phenomenon. According to Yin (2018), a “case” can sometimes be a person being studied, for example, a patient. Additionally, the “case” can also be an entity that is not clearly defined (Yin, 2018).

The case study can therefore form the boundary for studying programs, implementation processes or organisational change (Yin, 2018). The latter is relevant to this study because the investigation looks at the provincial government as the entity, intending to allow the participants to give in-

depth information about information security awareness. For this study, the residual organisational change would be to instil organisational ISC.

The nature of the case study, i.e. provincial departments in the Eastern Cape Province, is now introduced to the reader.

Figure 9: The Eastern Cape Province, South Africa (Encyclopedia Britannica Inc.)

The Eastern Cape is the second largest of South Africa's nine provinces. The map of the Eastern Cape is shown in figure 9 above. Located in the easternmost part of South Africa, Eastern Cape is an area of almost 170 000 square kilometres of diverse landscape. The provincial government head offices are located in Bhisho in the Buffalo City Metro. The Eastern Cape provincial government is composed of thirteen departments, namely: Community Safety, Cooperative Governance and Traditional Affairs, Economic Development, Environmental Affairs and Tourism, Office of the Premier, Education, Health, Human Settlements, Provincial Treasury, Public Works and Infrastructure, Rural Development and Agrarian Reform, Social Development, Sport, Recreation, Arts and Culture, Transport. These thirteen provincial departments are mainly around Bhisho. The researcher has identified two departments to be the focus of this study. These two departments are named Department 1 (D1) and Department 2 (D2) to maintain anonymity in the Eastern Cape provincial government.

A qualitative design to collect data from the two departments (Eastern Cape provincial government) to understand what was required to prepare an ISA programme was used by the researcher. The provincial government departments provided a relevant context for the research

aims, as the departments are challenged by information security audit reports (Eastern Cape Provincial Treasury, 2017; 2016; 2015; 2014).

Tang, Li, and Zhang (2016) warn that a case study can present challenges with respect to having sufficient rigour and reliability in information security research. Thus, to ensure that there is sufficient reliability, the researcher ensured that there are many respondents selected from the same department working in various units or directorates and whose backgrounds differ. Moreover, the respondents were requested to review the research results. A sufficient amount of data was gathered to be analysed. In addition, two provincial departments have utilised the case.

The research case consists of interviews of departments' units, IT managers, and employees. This approach is suitable, as the interest of this study is not focused on one particular user level but on how users' narratives reflect on information security risks and threats and on factors required for the preparation of an ISA program.

The interview guide questions were applied in the government context, where the respondents are employed. In addition, each provincial department selected has the following key characteristics:

1) Each department has an information security policy to guide government employees' security behaviour.
2) Each department is vulnerable to information security risks and threats.

These characteristics bring together key elements that must be consulted when conducting ISA, enabling improvement in information security behaviour and ensuring that employees comply with ISPs. These elements are the information security policy, information security risks, and threats. Together, these elements show a need to prepare an ISA programme. The case study is interpretive in its approach and aims to explore the insight of government employees on information security in the provincial departments.

The respondents were requested to voice their views in an interpretive manner that is not influenced by security processes that are currently in existence or not in existence. This will ensure that the findings from the participating departments give the perceptions of government employees 'level of information security awareness. This provides the specific requirements important to each respondent. Also, on the contrary, it implies that the researcher identifies even those items that seem to be less important. The case study then gives responses that are compared to one

another and then identify the trends. This then shows the detailed framework derived from a collection of information security data from the provincial setting.

When using a case study, an inclusive and full understanding of how complex a case can be is required. Stake (2005) asserts that the case study is built up using qualitative data, for example, observations, interviews, and documents. Firstly triangulation is done to clarify the meaning. Secondly, the researcher focuses on diversifying the perceptions through case study design by directly interpreting and categorically aggregating (Stake, 1995, p.74). The main aim of a case study is the understanding of the case. The reader of the research project should interpret it; hence the researcher has to provide the material sufficiently (thick descriptions) for the reader to learn from the case and enable the reader to make inferences from it. Readers can then generalise from the case study using their understanding and experiences ("naturalistic generalization").

The primary data collection process will be introduced in the next section.

5.5. Data Collection

A set of four identified themes was derived from literature to be the basis to derive the research instrument from collecting the primary data. These themes were then used to structure the questions that arose from the literature.

5.5.1. Study participants

The participants in the study are provincial government employees who carry out different roles, as indicated in Table 7. Twelve interviews were conducted with Department 1 (D1) and Department 2 (D2) IT-related staff. In each department, the participants were actively involved in the IT sections of the respective departments with the respondents including IT support staff and IT managers. The choice of 12 employees from D1 and D2 was based on the availability of the employees and their willingness to participate in the study. The data collection occurred during the COVID19 pandemic, with many staff working remotely, which increased the complexity in getting participants to volunteer to participate in the study.

Table 7: Study participants

Cases	**Participants**		
Department	**IT Managers**	**Employees**	**Total**
Department 1	2	4	6
Department 2	2	4	6
GRAND TOTAL	**4**	**8**	**12**

Purposive sampling was used in the two chosen departments. The reasons to choose the purposive sampling for this study are 1) the proximity of the participants to the researcher and 2) shared employee characteristics among the participants that fit what the study seeks to understand (Campbell et al., 2020; Sibona, Walczak, & White Baker, 2020). Identifying participants was easy as the researcher works in a provincial government department. The study participants were drawn from two of the five Eastern Cape Provincial Government departments IT sections. Individuals were selected based on the assumption that they possess knowledge and experience of how the information assets and resources of the Provincial Government are managed. Participants are chosen in a qualititative study to provide insight into the phenomeon for added detail (depth) and potential generalisability (breadth) to similar settings (Palinkas, Horwitz, Green, & Wisdom, 2013).

The participants were contacted by email with the permission of their Head of Department (HOD) once the government ethics approval had been received to allow the administration of the study with government employees. The identified participants were provided with the details of the research study and asked whether they would be willing to participate. The participants were advised that they were not required to complete the interviews by their HOD and could elect not to participate. Of the participants approached, some indicated their unwillingness to participate due to a perception of HOD authority or suspicion that the HOD would have access to their responses. The participants who agreed to participate did so on condition that their responses were anonymous and would not be shared directly with their repective HOD. The semi-structured interviews were then conducted using the research instrument.

5.5.2. Research Instrument

A research instrument is a guiding tool that assists the researcher in gathering, measuring, and analysing data related to the research topic of interest (Pazur, 2020; Phillips, 2017). The questions in the research instrument were structured in an interview schedule, which contained questions from each theme. The discussion informed the theme arising from the research sub-questions and theories that are the basis of the study.

The researcher checked and refined the research instrument through a pilot study.

5.5.2.1. Pilot Study

Since this research study is based on individual perceptions, (Blumberg et al., 2008) recommends using semi-structured one-on-one interviews to get each participant's perceptions on each given

topic. An interview guide approach guides the semi-structured interview and ensures that the research covers all the themes asked of the participants.

The rationale for conducting a pilot study is to assess whether the questions asked from the respondents are clear and easily understood, estimate the length of time for each interview and after the pilot study, and define the questions that were not clear (Ismail, Kinchin, & Edwards, 2018; Yin, 2018). The pilot study was conducted with one participant to confirm if the interview questions were clear and correct for semi-structured interviews. From the participant's feedback, tricky questions were reworked, the questions were then re-tested and rephrased based on the inputs from the respondent.

Revising Question 1.4.

When having strategic planning sessions, does your department include the protection of information as part of the discussions?

Prompt 1: What information security strategy (if any) is put in place to protect information assets?

The respondent felt the question was not easy to answer due to their limited knowledge/exposure to strategic planning sessions of the department. Therefore, if a respondent cannot answer this question, then a second prompt question would be asked of the respondent being interviewed.

Prompt 2: In your opinion, how can your department include the protection of information assets during the planning sessions?

Revising Question 3.3.

What is your experience of how your department deals with someone who does not abide by the information security rules as outlined in an information security policy, and there is a security breach?

Prompt 1: Have you ever heard of any such actions being taken against an employee in your department or another government department?

The respondent felt the question was not easy to answer because it is not implemented in the department yet. Therefore, the question was rephrased so that the answer would be more of speculation than reflecting an actual situation. Prompt 2 was also added to provide a richer response.

Suppose that in your department, security awareness of information security policy has been conducted and an employee does not abide by information security rules as outlined in the security policy, and there is a breach.

Prompt 2: What actions do you think the department should take against such an employee?

In addition, from the input from the pilot session, the researcher made some minor changes to the instructions until the participant agreed that the instructions were clear and expressed what the researcher intended to say. The interview guide (Appendix B / Figure 9.) was then finalised to administer in the semi-structured interviews.

Figure 10: Interview Guide

Research Instrument for the Masters Dissertation titled:

A framework to prepare an information security awareness and training programme: A case of the Eastern Cape provincial government

---

Interview preamble

The following questions focus on clarifying potential determinants of an Information Security Awareness program for Eastern Cape Provincial departments.

Interview Questions

1. Organisational Information security culture

What do you think of when you hear the term *information security*?
Prompt 1: How might information security be applicable in your personal life?
Prompt 2: How might information security be relevant in your work life?

1. 1 In your opinion, how important is *information security* in the management practices of your department?
Prompt 1: Are you able to provide some examples where management has raised issues around *information security*?
Prompt 2: Are you encouraged in the workplace to follow "good" information security practices provided by management?

1.1. What activities (if any) does your department do to promote *information security awareness* amongst its employees?
Prompt 1: Is an effort made to make employees aware of *information security* related policies, which might impact their daily job?
Prompt 2: Are employees made aware of any compliance requirements associated with information security policies?

1.2. When having strategic planning sessions does your department include the protection of information as part of the discussions?
Prompt 1: What information security strategy (if any) is put in place to protect information assets?
Prompt 2: In your opinion, how can your department include the protection of information assets during the planning sessions?

1.3. What continuity processes are you aware of if a disaster (human or otherwise) strikes the information assets of the department?
Prompt 1: Are you aware of any documented processes?
Prompt 2: Have any continuity plans been communicated to employees?

2. Information Security risks and threats

What is your specific role in the department, how do you perceive information security risks within your department?

2.1. Do you know where to get a copy of information security policies (if it exists) for your department?
Prompt 1: Have you read any rules or policies regarding information security?
Prompt 1.1: If no – prompt – is there any specific reason why you have not done so? Why not?
Prompt 1.2: If yes, were these understandable?

2.2. Have you been informed of information security requirements in the last twelve months?
Prompt 1: For example regulations regarding downloading of email attachments from unknown sources.
Prompt 1.1: If yes, how do you comply with these requirements?

2.3. What do you understand as an information security incident in the workplace?
Prompt 1: Are you able to share an example that may have happened in the last 12 months that you are aware of?

2.4. *Information security breaches occur when an intruder gains unauthorised access to your department's protected systems and data.* What measures are you aware of that your department is taking to ensure that there are no security breaches?

2.5. What information security threats are employees exposed to in relation to information assets?
Prompt 1: How does the department reduce information security threats?
Prompt 1.1: For example, weak passwords, or unauthorised installation of an application on the computer, or uninstalled updates?

3. Employees' perceptions about information security

3.1. How do you feel that employees can comply with the requirements of your department's information security policy?

3.2. What is your view on the measures put in place by your department to reduce the chance of information security threats?
Prompt 1: For example, some companies require staff to change a password on monthly basis?
Prompt 2: For example, are you able to download work related content and take it away from the office to work on it?
Prompt 2.1: How do you protect the data when it is in your possession?
Prompt 2.1.1: For example, from theft, unauthorised access?

3.3. Suppose that in your department security awareness of information security policy has been conducted and an employee does not abide by information security rules as outlined in the security policy, and there is a breach:
Prompt 1: What actions do you think the department should take against such an employee?

3.4. Do you think your department could be vulnerable to information security threats?
Prompt 1: What leads you to this conclusion?

3.5. How do you think an employee can become knowledgeable about information security policies and guidelines?

Prompt 1: Are there any aspects that you think might complicate employees getting the knowledge about information security policies in the workplace?

3.6. How confident are you that you can comply with information security policies?
Prompt 1: Why do feel that way?

3.7. What sanctions are in place by if information security policies are violated?
Prompt 1: If those sanctions are severe, are employees likely to change their information security behaviour? What makes you think so?

3.8. What can promote better security behaviour among employees in your department?

4. Security Awareness

What is your specific role in the department? How do you perceive the department's ISA programmemes

4.1. Does your Department conduct information security awareness training sessions?
Prompt 1 - **YES**: What types of topics are covered in the training sessions?
Prompt 1.1: Are you aware of your Department budgeting money and time for information security awareness related training?
Prompt 1.2: Is ongoing information security awareness training part of the employee development in your Department?
Prompt 1.2.1: How is it / should it be done?
Prompt 1.3: Is the training offered in-house by the Department or offered by an external vendor (outsourced)?
Prompt 1.3.1: If the training is offered by an external vendor, how is it tailored to your day to day job?
Prompt 1.3.2: What do you feel is the best way for training to be delivered to you in the workplace? For example, face-to-face training, online videos, computer-based training?
Prompt 1.4: How do you make sure that specific information security training is attended by relevant employees?

Prompt 2 - **NO**: What types of topics do you think should be included in such training if it were offered?
Prompt 2.1: What would you want to know more about - from an information security point of view?

Thank you for taking the time to help me understand your working environment and the impact of information security awareness.

5.5.2.2. Administering the Interview Guide

Each interview lasted between 40-60 minutes and was conducted by the Microsoft Teams virtual meeting platform. The software allowed for the recording of the sessions with the permission of the participant.

The responses provided by the respondents form the primary data of this study. This study used semi-structured interviews as the main data collection technique. Semi-structured interviews have characteristics of both structured and unstructured interviews and have closed and open questions. The researcher had to provide pre-planned main questions to guide the respondents. This is done

to maintain consistency with all the interviewees. The participants were encouraged to give more information when they wished to do so.

The interview guide required respondents to provide an opinion answer. Therefore, the response given is a respondent's personal opinion on the knowledge of information security awareness of the department. The interviews were conducted over some time in two separate stages. In the first stage, the respondents from the first department (IT managers and employees) were interviewed, and they were open about discussing the current practices of their department from their perspectives. In the second stage, the respondents from the second department (IT managers and employees) were interviewed.

Participants were advised to give their independent views to all questions asked from them. Sharing their personal views in answering the questions satisfies the qualitative component of the research methodology. These questions were open-ended, and the respondents needed to provide answers that reflected their daily practices and routines.

The responses from twelve respondents were collected from the semi-structured interviews that were conducted. Once the interviews were complete, the researcher stored the recordings for later data analysis.

5.6. Data Analysis

The first step was to explore the narrative of the 12 interview transcripts. The researcher explored the transcripts by reading the transcripts thoroughly several times, with the intention of capturing the specific themes and reviewing employees' answers as a whole. Adding up on these first main categories, the researcher coded continuously for all the interviews, developing main categories using content analysis (Miles, Huberman, & Saldana, 2018). The researcher made use of the MS Excel spreadsheet software to code, sort, and categorise the responses of the participants.

After the researcher completed the coding, the researcher started discussing the main categories and mutually validated the codes, internally and externally (Linneberg & Korsgaard, 2019; Yin, 2018). Chronologically, this study is building on a repetitive process that relies on data and theoretical insights from the literature to formulate propositions that reflects a deductive and inductive approach, putting together conceptual insights.

There is no personal information that is needed during the data analysis (Harding, 2018). Departmental information security awareness level is more significant for this study, more than

the identity of the department. The results from data analysis were used to create an information security awareness program.

5.7. Ethical Considerations

This section explains how the researcher considered ethics while conducting the study. The focus of the research project was the preparation of an information security awareness program for government employees which was firstly developed from reviewing the existing literature. The researcher needed to get a gatekeeper approval letter from Provincial Government departments to conduct research. The participants in this research (respondents) were informed about the intentions of this study in order to allow them to decide whether they would voluntarily participate or not. Every participant was treated anonymously, and the interviews were done on a voluntary basis. During the interview process, the respondents were informed they were not obliged to answer any given question and had an option not to answer if they so felt. Moreover, the respondents were advised that they would be kept anonymous and their responses confidential if they so desired. These ethical considerations were also included in the research proposal of this study, and the Ethical Committee has granted permission for this study. The Ethical Clearance number is BOU021SPOT01 (cf. Appendix A: Ethical Clearance Certificate).

5.8. Research Evaluation

In ensuring that the research project is credible and has integrity, the research evaluation becomes an essential step. According to Korstjens and Moser (2018), there is a set of equivalent criteria for interpretivist research. These are shown in Table 8.

Table 8: Quality in Interpretivist Research (Oates, 2006)

Interpretivism
Trustworthiness
Confirmability
Dependability
Credibility
Transferability

The interpretivist criteria apply to this research as follows:

- **Trustworthiness**: Lincoln and Guba (1985) proposed use of terms such as credibility, transferability, dependability, and confirmability in qualitative research to ensure "trustworthiness" of the study.

- **Confirmability**: This criterion has been met through the use of multiple data collection techniques – secondary and primary data. In addition, the researcher bias is seen to be mitigated through the verification of the data by confirming the findings and arising inferences with the presented literature. Furthermore, confirmability arises by verifying whether the findings are understood to be originating from the data and setting (Moon, 2019), which was done in the discussion of the findings.
- **Dependability**: To achieve dependability, the researcher reports the processes performed in the study in a detailed manner so that other researchers in the future can repeat the study and get similar results (Lishner, 2015). The research process followed in this study has been explicitly detailed, for example, by using literature from recognised sources or authors and using well-known theories and frameworks which in have previously been empirically tested. The theories and frameworks that have been used in the research projects include the Organisational Culture Theory, Protection Motivation Theory and Information Security Culture Framework. In addition, the research process has been clearly documented, so that the methods followed can be applied to a similar setting to confirm whether the findings are similar.
- **Credibility**: *Credibility,* according to Merriam, as quoted by Shenton (2004), is the qualitative investigator's counterpart that answers the question, "How congruent are the findings with reality?" (p.64). To ensure credibility, after interviewing the respondents using the interview guide, the researcher can taken the transcript back to interviewees to verify the correctness of data (Lemon & Hayes, 2020). The researcher in this study completed the transcription and then approached the participants to confirm that the information as transcribed was accurate as per their recollection from the interview.
- **Transferability**: Transferability has been achieved by making use of a multiple case study approach that will enable transferability of findings which will make it possible to apply the study to other public sector settings with similar features (Fusch, Fusch, & Ness, 2018). The researcher conducted the interviews with two comparative IT sections from two different provincial government departments for compariative purposes. The comparisons between the departments are presented as part of the findings chapter.

By applying the five criteria, the researcher has observed the integrity and credibility of the research project.

It is also important to note the concerns of the positivist with regard to the disadvantages of using the interpretive approach when conducting research (Moon, 2019; Oates, 2006). The following are shortcomings raised by positivists on interpretivism:

- ***Objectivity*** – the positivist argues that there is no researcher bias, whereas the interpretivist is cautious of his or her bias when conducting research.
- ***Reliability*** – the positivist mentions that repeating research experiments is a cause of research quality, while interpretivists maintain that theenviromnet, where the research is conducted, keeps on changing and, therefore repetition, is elusive.
- ***Internal validity*** – The positivist will rely on causality where all variables are assumed to be known, whereas the interpretivist embraces the unknown and subjective nature of reality.
- E***xternal validity*** – the positivist strives for the goal of being able to generalise the research findings, whereas the interpretivist realises that the uniqueness of situations may make generalisation unlikely.

There are shortcomings when interpretivism is judged against positivist criteria for arriving at the truth of a given phenomenon (De Vos, Strydom, Fouche, & Delport, 2005). Thus, it is worth noting that "qualitative and quantitative methods rest on different assumptions and have different purposes" (Martella, Nelson, & Marchand-Martella, 1998, p.295). However, Oates (2006) concedes that the interpretivism approach to research increases the body of knowledge within the information systems studies.

5.9. Conclusion

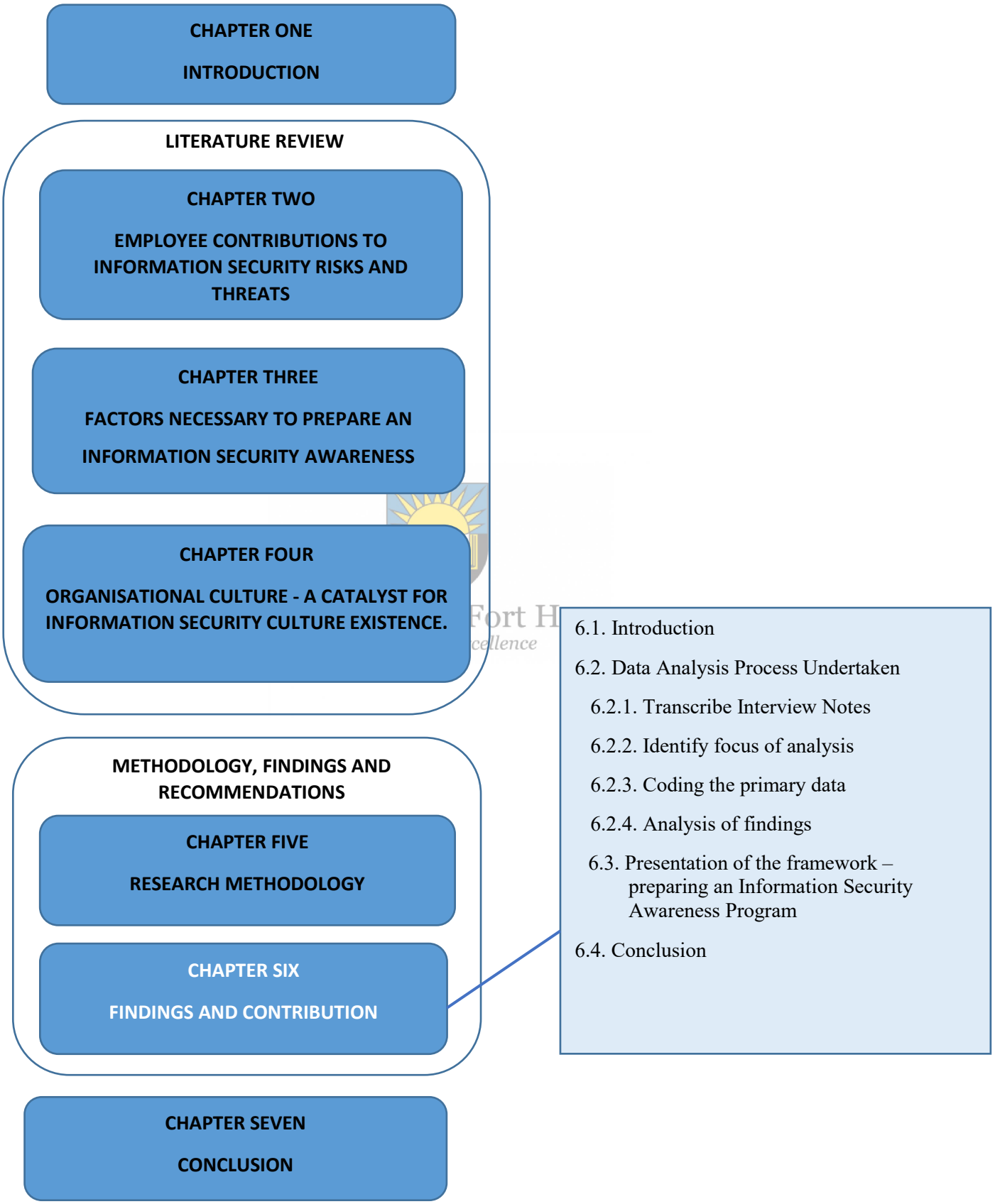
The research methodology chapter becomes very important as the researcher has to prove that the study was has been undertaken systematically. The research paradigm of this research project was established to be that of an interpretive paradigm and was compared to that of the positivist paradigm. From the interpretive paradigm, the reality of the study is through social concepts such as perception and collective meaning. This enables respondents, through their subjective opinions, to interpret their individual understanding of information security in relation to activities performed by employees to address information security risks and threats, awareness and culture. Thereafter, a brief comparison of qualitative, quantitative and mixed methods was made. The research methodology was established using the qualitative method. The qualitative approach

ideally suited this study because of the value of a person's natural ability to talk and the ability to provide insight into the social and cultural background on the topic of information security that is not taken into account in quantitative methods. This ties into the qualitative method through interview question statements utilised in the Interview Guide of each case study.

A pilot study was conducted to ensure that the questions prepared for the interviews resulted in accurate responses. Once the recommendations of pilot study participants were implemented, online semi-structured interviews were then conducted as the research instrument for this research project. Finally, sources of primary data, as well as secondary data, are discussed.

The next chapter discusses how the data that was collected from the respondents is analysed so that the researcher can articulate the process of preparing the information security awareness programme.

CHAPTER SIX: FINDINGS AND CONTRIBUTION



6.1. Introduction

The literature review discussion (*cf.* Chapters Two, Three and Four) made it possible to have all the key themes necessary to investigate the development of the conceptual framework. The derived artefact is a framework to assist Eastern Cape government departments in preparing an information security awareness and training programme. Chapter Five outlined the research process to collect and analyse the primary data from the study participants (IT Managers and end-users) through semi-structured interviews.

The next step was to code and analyse the responses by using themes identified in the literature review. The analysis process (Figure 10.) begins after administering the interview guide and the transcription of the responses from the respondents. The data was then analysed using the predefined themes generated from the key area of focus from the literature review. To elaborate on the statement made when explaining a theme, direct quotes of responses are occasionally given to clarify a point or support the discussion.

A presentation of the final framework proposed for this study is then made, incorporating the respondents' comments and views when the semi-structured interviews were conducted. The last section of this chapter will present and explain the *Framework for Preparing and Information Security Awareness and Training Programme*.

6.2. Data Analysis Process Undertaken

One of the requirements to conduct qualitative research is that the data analysis must be logical in explaining the process of data collection and analysis (Silverman, 2011). The method of collecting and analysing the data should be presented so that the reader of a qualitative study can follow the reasoning of the research project.

Figure 11 shows the step-by-step analysis process followed after the data collection initiated by the interview guide. The analysis process has four stages that guide how the information is interpreted. The stages done to analyse the data of the study are discussed in this section. A set of identified themes was made to be the basis to interpret the data that was collected. The themes used for categorising the responses stem from a combination of the three study research sub-questions, the two theories and the literature that has been reviewed and then discussed in terms of an information security awareness programme.

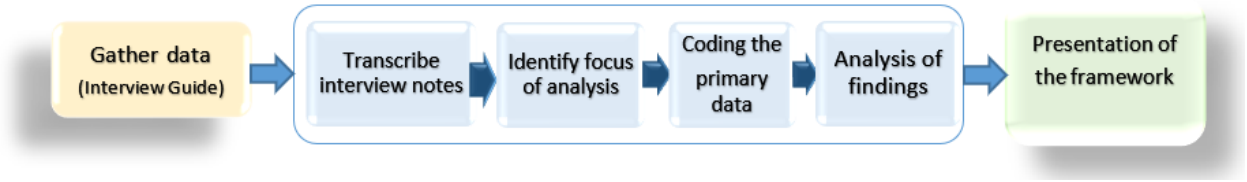


Figure 11. : The data analysis process applied in this study

The following sections discuss the process undertaken to analyse data in this study, as shown in figure 11 above.

6.2.1. Transcribe interview notes

The researcher gains familiarity with the data by transcribing the interview notes and/or recordings to facilitate the primary data analysis and enable information sharing with other people in a written dissertation (Moore & Llompart, 2017). The aim is to capture how the respondents uniquely told their stories and balance that with producing an accurate transcript (Nestel, Hui, Kunkler, Scerbo, & Calhoun, 2019). Therefore as a researcher, the following are the considerations to be noted when transcribing notes (Nestel et al., 2019):

- The approach decided upon by the researcher should be aligned with the research methodology.
- Symbols used in transcribing to express verbal and non-verbal cues must be easily understood to manage and analyse the datasets.
- There should not be any speaker labelling in the transcript other than some assigned key. This can be done by: (a) removing any identifying information (participant names, role, gender, and demographic data) to reduce bias and ensure confidentiality.

The researcher took note of the considerations and applied them when transcribing the primary data.

The researcher collated the recorded interview notes from the participants in the semi-structured online interviews. Where respondents responded in vernacular (IsiXhosa), the researcher translated the utterance into English and added the annotation [X to E] after the transcribed text. During the interview session, a few respondents would randomly change from English to isiXhosa to emphasise a certain point.

6.2.2. Identify focus of analysis

Robson (1993) stated that the purpose of analysing data is to reduce unnecessary data. Yin (2018) supports this statement by adding that identifying the focus of analysis assists the researcher plan and focus on the most relevant data.

The aim of collecting primary data for this study was to consider the discussion from the literature review regarding information security awareness and contextualise it within the department settings of the provincial government of the Eastern Cape.

The data analysis focused on integrating the semi-structured interview questions given to respondents and the themes from the literature. These were plotted to the data gathered using Excel. The assigned codes then guided the analysis write-up.

6.2.3. Coding the primary data

The reason to code the transcribed text is to analyse the primary data by linking the respondent utterances to the thematic areas of the research to allow for an analysis of the comparisons and differences (Silverman, 2011). The codes used to analyse the data were predefined and generated from the key areas of focus of the study (themes). The themes evolved out of the research focus of the study, the applied theories (the Organisational Culture Theory and the Protection Motivation Theory), and the literature discussion. The themes, code, categories and descriptions are included in Table 9. The codes generated from these themes were then assigned to the interview responses by the respondents in the two departments and mapped using Ms Excel. Table 9 includes the categories that apply to the relevant theme and form part of the write-up. How the thematic codes assigned in Table 9 were dispersed across the interview guide are indicated in Table 10, with one instance of each code being presented in the table.

Table 9: Allocation of Thematic Codes

No.	Theme	Code	Categories	Description
1.	Identifying Organisational Information Security culture	OS	1.1. Commitment of Top Management	The organisational ISC theme is about assessing the provincial departments' current organisational ISC. This involves looking into the organisational processes that promote information security policy compliance by employees, whether protection of information is one of strategic planning discussion or if employees are made aware of continuity processes in the case of a situation where information assets are struck by disaster.
			1.2. Existence of Information Security Strategy	
			1.3. Allocating of Information Security Awareness and Training Funding	
			1.4. Communicating of Continuity Plans	
			1.5. Enforcement of Information Security Accountability	
2.	Identifying Information Security risks and threats	RT	2.1. Incorporation of ISP into the new hire process	The information risks and threats theme looks at whether the employees understand the information security risks and threats they are exposed to and whether they are informed and updated on information security requirements, including security policies. This theme checks whether employees read rules and policies regarding information security and would be aware of the measures by the department to ensure that there are no security risks and threats.
			2.2. Access to ISPs and Minimum Information Security Standards (MISS)	
			2.3. Classification of Organisational Information *(Top Secret, Secret and Confidential)*	
			2.4. Update employees on new incidences	
			2.5. Notification of recent information security breaches and threats	
			2.6. Establishing Information Security Protocols for Remote Working	

No.	Theme	Code	Categories	Description
3.	Understanding Employees' Perceptions about information security	EP	3.1. Compliance with Information Security Policies	Employees' perception of information security focuses on their departments' views and feelings of information security. Whether they feel they can comply with security policies as required and therefore reduce security risks and threats. The employees should know how the departments deal with non-compliance to ISP, which results in security breaches. The employees also express what they feel can promote better security behaviour in the department.
			3.2. Simplification of information security policies and procedures	
			3.3. Reduction of chances of information security threats	
			3.4. Reinforcement of good information security behaviour	
			3.5. Sanctions for Non-compliance of ISPs	
4.	Conducting Information Security Awareness and Training	SA	4.1. Customised Information security awareness and training modules	The theme's focus is that the departments conduct information security awareness and training sessions, ensuring that the types of topics suitable for a particular audience are prepared for the security awareness training session.
			4.2. Listing of relevant information security awareness and training topics	

Table 10: Application of the thematic code to the interview guide questions

	Semi-Structured interview guide questions	Thematic Code
1.1	What do you think of when you hear the term *information security*?	**OC, EP, RT**
1.2	In your opinion, how important is *information security* in the management practices of your department?	**EP, OC**
1.3	What activities (if any) does your department do to promote *information security awareness* amongst its employees?	**OC, SA**
1.4.	When having strategic planning sessions, does your department include the protection of information as part of the discussions?	**OC, EP**
1.5.	What *continuity processes* are you aware of if a disaster (human or otherwise) strikes the information assets *of the department?*	**OC, RT, EP. SA**
2.	What is your specific role in the department, how do you perceive information security risks within your department?	**EP, RT**
2.1.	Do you *know* where to get a copy *of information security policies* (if it exists) for your department?	**EP, RT, OC**
2.2.	Have you been informed of information security requirements in the last twelve months?	**RT, SA, OC**
2.3.	What do you understand as an information security incident in the workplace?	**RT**
2.4.	What measures are you aware of that your department is taking to ensure that there are no security breaches?	**RT, SA, OC,**
2.5	What information security threats are employees exposed to in relation to information assets?	**RT, OC**
3.1.	How do you feel that employees can comply with the requirements of your department's information security policy?	**EP, SA, RT, OC**
3.2.	What is your view on the measures put in place by your department to reduce the chance of information security threats?	**EP, RT, OC**
3.3.	What is your experience, of how your department deals with someone who does not abide by the information security rules as outlined in an information security policy, and there is a security breach?	**EP, RT, OC**
3.4.	Do you think your department could be vulnerable to information security threats?	**EP, RT, OC**

3.5.	How do you think an employee can become knowledgeable about information security policies and guidelines?	**EP, SA, RT, OC**
3.6.	How confident are you that you can comply with information security policies?	**EP, RT**
3.7	What sanctions are in place by if information security policies are violated?	**OC, RT**
3.8.	What can promote better security behaviour among employees in your department?	**OC, SA, EP**
4.	What is your specific role in the department? How do you perceive the department's ISA programmemes	**EP, SA**
4.1.	Does your department conduct information security awareness training sessions?	**SA, OC**

To better understand the prevalence of the allocation of the thematic codes to the codified data, a tally of each code allocated to the respondent responses was made with the information presented in Table 11. Tallying the thematically coded responses assisted the researcher in understanding where the majority of responses were grouped. The coded responses were arranged most prevalent to least prevalent. The list of responses grouped show EP (*employee's perceptions about information security*) as the most frequently occurring response from question 1 to question 4 from the interview guide. The thematic code SA (*security awareness)* has the least assigned responses from the interviews. The low SA ranking was confirmed based on the current lack of security awareness training sessions being conducted by Departments. The staff interviewed were not aware that such training was being communicated or run by the relevant Department.

Table 11: Number of statements (responses) given to a specific theme code by (prevalence)

Theme Code	Number of statements (responses)
EP	88
RT	66
OC	55
SA	11

The following sub-section discusses the findings of the study based on the responses provided by the provincial government employees by framing the discussion within the themes (*cf.* Table 9).

6.2.4 Analysis of findings

As stated (*cf.* Chapter 5), the study sought responses from a sample of staff (IT managers and employees) in two provincial government departments in the Eastern Cape Province. The participants and their originating Departments in the study were anonymised to ensure that the responses could not be traced directly to an individual staff member. Table 12 indicates the identifier (key) that was used to identify respondents utterances.

Table 12: Allocation of Setting & Respondent Keys

Setting & Participants	Assigned identifier (key)
Department	D1, D2
Respondents	R1, R2, R3, R4, R5, R6, R7, R8, R9, R10, R11

The identifiers (Table 12) will be used to differentiate the utterances from respondents under each of the thematic areas and categories (*cf.* Table 9). The discussion of the findings is related to the responses and the literature and lead to recommendations.

6.2.4.1. Theme 1: Identifying Organisational Information Security Culture (OC)

The organisational culture must show a good attitude towards information security for the whole organisation (Ashenden, 2018). It is also key that the activities performed in the Eastern Cape Provincial Departments be consistent with the practices of a good ISC (Amankwa, Loock, & Kritzinger, 2018; Palega & Knapinsski, 2019). Hence the management of the Eastern Cape Provincial Departments must establish a security culture within the organisational culture (Karlsson, Denk, & Åström, 2018). It is the responsibility of the top management to create an environment of learning the values of the organisation for its employees and help them to be capable of complying with ISPs to improve compliance (Shouran, 2019; Thomson & Van Niekerk, 2011). This theme is closely linked to Theme 4 as it is also concerned with the Eastern Cape Provincial Department's culture as an organisation in promoting security awareness. The Organisational Information Security Culture theme will be analysed in terms of the respondents' responses and be grouped according to the sub-categories identified (*cf.* Table 9).

6.2.4.1.1. Commitment of Top Management

As mentioned (*cf.* section 4.5.1), one of the effective ways to cultivate and reinforce a culture is to consider what leaders pay attention to, measure and control. If employees don't see security being taken seriously by upper management, they cannot be expected to be serious about security awareness matters (Bemis, 2017). The top management of the Eastern Cape Provincial Departments that expresses its expectations, entrench them gradually and continually in the organisation's vision, mission, goals, structures and employees' activities (Nel & Drevin, 2019).

The respondents, when asked about their opinions on the importance of information security in the management practices of their Eastern Cape Provincial Departments, made the following comments:

"Management doesn't take information security seriously, at least not at our department or even every other department that I have worked at" **(R1)**

"I would say the management is fully aware of how information security operates and how it assists an organisation, but in terms of implementation, I don't think they are fully implementing it to its optimal level". **(R3)**
"It should be a very important part. I'm not sure whether our department understands […]". **(R2)**

"It is not a discussion that happens every day as it should. It's not a topic that becomes an agenda item regularly in the management space". **(R7)**

The responses are from staff in both Eastern Cape Provincial Departments (D1 and D2) and indicate that there is lack of management commitment from top management to regularly engage with staff on information security issues..

To prepare the ISA programme for a department, there needs to be a sign-off and commitment from Top management of each Eastern Cape Provincial Department, that raising information security awareness is a critical agenda item.

6.2.4.1.2. Existence of Information Security Awareness Strategy

Organisations with an information security awareness training strategy have lower security incidents than those who do not train their staff (Labuschagne, 2017). Therefore the executive management of the Eastern Cape Provincial Departments needs to establish the expected culture by outlining the information security awareness strategy of the Eastern Cape Provincial Departments (Hu, Dinev, Hart, & Cooke, 2012). Information protection is a strategic risk management issue for organisations of all types and sizes (Labuschagne, 2017). There is often no detailed and solid security strategy where the Eastern Cape Provincial Departments can draw on clarity and consistency. The respondents gave the following response when recalling whether the Eastern Cape Provincial Departments include protection of information as part of the discussion when having strategic planning sessions:

"*No. It's only when it is not in the strategic planning. When it has been discussed in another committee or in that forms, but in terms of when it's a planning session, there's never been a session for information strategy, so there's no strategy around information security"* **(R2)**.

Another respondent confirmed this sentiment and said,

> *"I'm always there, and I know, but it doesn't happen to that extent. What happens is[X to E] because you will have people from IT discussing their own spaces they discuss their plans [X to E] and things that they are going to be doing-especially in supporting other departments and other people, but it is not a matter of us saying how do we then prioritise information security in the department, it does not become an indicator that gets lifted up such that it is given that weight [X to E] that it deserves"* **(R7)**.

(R6) had also shared the same comment

> "*No. Not that I recall".*

There was no significant difference between responses from respondents from D1 and D2. There is a lack of robust organisational security strategy. Based on the responses from D1 and D2, and supported by literature, to prepare an ISA programme, the information security awareness strategy should be developed and implemented in the Eastern Cape Provincial Departments.

6.2.4.1.3. Allocating of Information Security Awareness and Training Funding

Providing an information security budget is linked to having an information security strategy in place (*cf.* section 3.6). An organisation might be challenged with not clearly defining funding for the training and awareness programme (Dhakal, 2018). The Eastern Cape Provincial Department's executive management must support the programme and decide on the security awareness and training budget (Wilson & Hash, 2003).

According to Sarala et al. (2016), the Eastern Cape Provincial Departments should have an information security officer responsible for managing and highlighting information security and controls aspects. Firstly, Sarala et al. (2016) assert that selecting the controls must be done such that the cost of the chosen controls have to be within the budget limits of the Eastern Cape Provincial Departments and should not be above the losses incurred by the organization. Secondly, it must be done to address the vulnerabilities and mitigate risks that remained unresolved. The suggestion from a respondent highlights the importance of appointing a dedicated qualified information security specialist in the Eastern Cape Provincial Department

> *"I think that they can comply if the department can invest in security because we need that security specialist in the department*" **(R4).**

Respondents from both **D1** and **D2** implied the challenge of not allocating funding for information security. Based on the literature and responses from the respondents, to prepare the ISA and training programme in a provincial department, there needs to be an annual budget allocation dedicated to conducting ongoing information security awareness, including resourcing all information security requirements.

6.2.4.1.4. Communicating of Continuity Plans

The Business Continuity Plan should be available online and within easy reach through the Internet to appropriate employees when the need arises (Whitman & Mattord, 2018). This plan documents actions taken by the top management to elaborate what efforts will the Eastern Cape Provincial Department make if a disaster strikes the organization's primary operating location (Whitman & Mattord, 2018). This is supported by literature (*cf.* section 3.6) stating that awareness should be informed by the organisation's perceived threats (Amjad, Naeem, & Zaffar, 2016).

Respondent **(R2)** mentioned:

> *"We still have to develop a proper disaster recovery plan. So it is not documented."*

The respondents were unable to draw an informed conclusion as to whether continuity documented processes existed or if they were simply not being communicated to employees, and the responses ranged from,

> *"We are immature in that sense"* **(R8)** or *"they are not documented"* **(R5)**, and *"No, it is not communicated to employees"* **(R3)**.

The respondents from both D1 and D2 echoed the same response that they are not aware of any continuity processes if a disaster strikes the information assets of the Eastern Cape Provincial Department, nor do they know any documented processes or plans communicated to employees. To prepare an ISA programme, the Eastern Cape Provincial Departments should adopt an ISC of sharing the business continuity plan so that any appropriate employee can access these plans when the need arises.

6.2.4.1.5. Enforcement of Information Security Accountability

The attitude of employees towards the E.astern Cape Provincial Department's recommendations of the ISA programme depends on the sanctions for non-compliance as stated in the ISA programme (Bada and Sasse, 2019). Additionally, the Protection Motivation Theory proposes that what motivates employees to comply with information security policies emanates from what the employees perceive as a threat of complying or not complying with information security policies, and also avoiding the negative consequences of not complying or complying with security activities (Bauer, Bernroider, & Chudzikowski, 2017)

The respondents had this to say about enforcing information security accountability

> *"I think accountability and consequent management"* **(R11)**.

The respondent, **(R1)** also confirmed this:

> *"I think definitely education, awareness and then visible sanction for non-compliance*".

The respondent, **(R8)** advised:

> *"Communication, communication enforce it. Send it out. Warn the people. You know it must be in their faces all the time. Not once a year, but be there every time, prompts on the laptops."*

The respondent **(R1)** suggested utilising the already existing *Code of Conduct* document for public servants to provide a framework for sanctions.

In both Eastern Cape Departments D1 and D2, there were no significant differences in views by the respondents on the enforcement of information security accountability. Based on the participants' responses and literature, to prepare for the ISA programme, there needs to be an organisational ISC that enforces information security accountability. This can be facilitated by incorporating information security awareness in the Code of Conduct document of the Eastern Cape Provincial Departments with clearly defined sanctions for non-compliance.

6.2.4.2. Theme 2: Identifying Information Security Risks and Threats (RT)

This theme is concerned with whether the employees' compliance with information security policies and procedures leads to reducing security risks and threats (Bauer, Bernroider, & Chudzikowski, 2017). The employees should understand the nature of information security risks

and threats that they are exposed to (*cf.* section 2.3). Applying a policy is one of the defence control strategies to reduce the security risks (Whitman & Mattord, 2018). A policy defines right and wrong, the penalties for violating policy and the appeal processes (Whitman & Mattord, 2018). The employees should be informed and updated of security requirements (including ISPs) and read rules and policies regarding information security (*cf.* section 2.4).

The Information Security Risks and Threats theme will be analysed in terms of the respondents' responses and be grouped according to the subcategories identified (*cf.* Table 9).

6.2.4.2.1. Incorporation of ISP into the new hire process

In ensuring that employees are informed of the information security requirements, it is recommended that these security requirements of the Eastern Cape Provincial Department from the employees are included in the process for all new hires (PCI security Standards Council, 2014). When incorporated into the new hire process, the Eastern Cape Provincial Department will ensure that security awareness and training objectives are marketed without necessarily relying on the commitment to do so by each unit in the organisation. Top management support, therefore, becomes crucial (PCI security Standards Council, 2014).

The respondent opined that,

> *"All policies relating to information security should be read and signed at the time of joining the organisation"* **(R1)**.

The respondent shared the same view that,

> "*During induction of newly appointed employees, the department should inform or induct newly appointed employees of the security requirements"* **(R9).**

There was no significant difference between **D1** and **D2** regarding the responses of the respondents in this category.

Based on the responses from the respondents and the literature, to prepare the ISA programme, the Eastern Cape Provincial departments should include information security practices as part of the induction programme of newly appointed employees in the Eastern Cape Provincial Departments.

6.2.4.2.2. Access to ISPs and Minimum Information Security Standards (MISS)

Employees' knowledge of information security policies has a good effect in changing employees' attitudes towards complying with ISPs (Soomro, Shah, and Ahmed, 2016). However, most employees are not aware that the ISPs exist in their provincial departments because they are not made available for everyone to access them (Aloitabi, Furnell, & Clarke, 2016). Employees must comply with ISPs to reduce information security incidents (Bauer, Bernroider, & Chudzikowski, 2017).

The majority of the respondents are confident that employees can comply with their department's information security policy requirements if they are made aware of security policy.

Respondent **(R9)** stated,

> *"If there's an information security policy, it needs to be communicated; it must not just be there and not communicated. You can't just develop that policy, and then it sits there. "You have to workshop people and communicate it to people. You have to make sure that when you have communicated the policy when there are incidents, you address these things and over and above having to make sure that you bridge the gap you correct things."*

The respondent **(R1)** made the following comment about a place to get a copy of ISP and whether the respondent read the policy,

> *"It is not widely published ... we have to publish our policies on the intranet website where everybody has access to them. I believe that people might go and read them. If it exists, it is probably residing with the Strategic Management unit. Not in our unit".*

A slightly different response from another respondent **(R2)** was

> "*the old ones exist. We have recently done a user access policy. So we are waiting for that one to be approved".*

Another respondent **(R3)** also commented on seeing a recent draft security policy being circulated.

> *"I got a copy of that draft policy, but it was not detailed because there were lots of issues that needed to be tackled in that draft policy. It was not as comprehensive as one would want it to be*."

Other respondents stated that they had no idea that it existed. The employees must be aware of the Eastern Cape Provincial Department's measures to ensure that there are no security breaches and how the provincial departments reduce information security threats.

The Eastern Cape Provincial Department should have informed employees to comply with the information security requirements at least annually. The respondent **(R5)** and **(R3)**, respectively, commented

> *"Absolutely not. I 've never been informed."; "no, I haven't".*

The respondents mentioned that they were not told what was required regarding information security, which meant they were unaware of how to comply. The respondents from D1 and D2 said problems relating to access to ISPs and the MISS document. The Minimum Information Security Standards document is a national information security policy.

To prepare the ISA programme, there should be an awareness session related to ISPs by the Eastern Cape Provincial Departments through various delivery methods (*cf.* Table 4). Studying the MISS document should be enforced through a short course at the National School of Government (NSG).

6.2.4.2.3. Classification of Organisational Information (Top Secret, Secret and Confidential)

The Minimum Information Security Standard (MISS) was developed as an official government policy document on information security that must be complied with ***by any organisation handling classified information*** of the country (Michalsons, 2017). The most significant information security risk that is directed to organisations is posed by its employees (Giandomenico & De Groot, 2018). Employees' mistakes can easily lead to the revelation of classified data (Whitman & Mattord, 2018). Leaving classified information in unprotected spaces creates a vulnerability and, therefore, an opportunity for an attacker (Whitman & Mattord, 2018). Any data for public consumption and thus not classified should be marked (Whitman & Mattord, 2016).

Respondent **(R2)** commented that,

> "*You have to classify your information. The other information you publish and the other you cannot give out to other people. There is information the department keeps that is private or confidential and in the classification of information will determine how much security the department attaches to it."*

Another respondent **(R6)** also commented that,

"If a document is carrying information which is confidential in terms of classification, it means that document must be kept in a locked steel cabinet."

Respondent **(R6)** expressed the view that,

"*I do not believe users understand what is classified and not classified, and I think if you don't understand what is sensitive information and not sensitive information you'll never know what to protect or what not to protect you'll never know what it is that you are at risk of losing until you know the value that you've placed on that is. So I think you know we've got a long way to go before we get to the point where people actually start thinking about hey this document that I'm leaving here on my desk is that information that's a risk to our department."*

Drawn from responses from both D1 and D2, similar problems are happening in both Eastern Cape Provincial Departments.

Based on the responses from respondents and literature, to prepare an ISA programme, the Eastern Cape Provincial departments need to develop and implement a *Clean Desk policy*. The clean desk policy is a crucial organisational control policy that is meant to make sure that classified information is safeguarded daily (Djerouni, 2019).

6.2.4.2.4. Update employees on new incidents

Eastern Cape Provincial Departments need to keep employees informed about new incidents to prevent future similar events from occurring (Bada & Sigurdsson, 2020).

Respondent **(R6)** suggests that staff need to be kept informed

"we must be kept abreast of what is happening in terms of security threats" **(R6)**.

This suggestion was echoed by another respondent **(R4)**

"anything that will inform employees of what is happening out there because security breaches they happen into other provinces, other departments and in private sector. Some of them we have not experienced them yet, but that doesn't mean we will not experience them. So those experiences need to be shared with employees to understand the importance of a security awareness program. Once they know the seriousness of protecting information, then they will partake in the protection of information assets".

This suggestion is aligned with the literature (*cf.* section 3.3.1.4), stating that special attention should be given to advancing technology with new threats appearing; ICT infrastructure and

changes within the organisation. There should be continuous improvements in the ISA programme informed by these changes.

Employees showed their understanding of the meaning of information security incidents in the workplace which was evident from the explanation given by the respondents as they also shared an example that had happened in the last 12 months.

Respondent **(R1)** gave this explanation

> *"security incident is a vulnerability that has raised its head where information has either been leaked, stolen, altered and it has been done with purpose, and it has been done maliciously."*

The example given by respondent **(R3)** was more physical,

> *"Fire erupted at my department at the main building, and hard copy documents were burnt."*

From the responses from both D1 and D2, similar challenges are found in both departments.

In order to prepare the ISA programme, the Eastern Cape Provincial Departments should update employees when a new incident occurs in a Provincial Department.

6.2.4.2.5. Notification of recent information security breaches and threats

It is good to train employees to spot and report information security attacks (Bada & Sigurdsson, 2020). The Eastern Cape Provincial Department may offer employee training, and testing employees with simulated information security attacks can help stop many attacks and can help identify vulnerable users (Bada & Sigurdsson, 2020).

Respondent **(R6)** had this to say about being informed by the Eastern Cape Provincial Department's IT unit of new security breaches and threats,

> *"[…] When you are talking about individual person's information security, people are using ATM cards. People should be made aware of what is happening, what scams are around now, and all that stuff, but you do not get it with our IT unit, who are supposed to be doing that."*

The information threats employees are exposed to, according to **(R2)**, is that

"People will be walking around with USB and plug and play the movies and other data in the USB. I think we are not educating our users enough in terms of actual information security or lack thereof. Maybe we do it on a very small scale. Because when users take their computers home, and the antivirus is not updated, it may infect the computer and information assets of the department".

The other security threats that employees are exposed to, as given by respondent **(R1)**, are *"external access to information, clean desktop external workers coming to buildings, people carrying out things I mean we've lost computers in boardrooms, we've got systems administrators that aren't applying patches at regular intervals, we don't run security analysis, threat analysis on our networks at regular intervals, we don't get external companies to come and do security analysis and group force simulations."*

Drawing from the respondents' responses from both D1 and D2 and literature, the Eastern Cape Provincial Departments are not giving updates on the latest security breaches that have just occurred. To prepare the ISA programme, there needs to be a system of notifying employees of the recent information security breaches and threats.

6.2.4.2.6. Establishing Information Security Protocols for Remote Working

Controlling security and privacy can be a serious challenge if employees and their working machines are not physically in the building (Bada & Sigurdsson, 2020). The respondents shared their views on the measures put in place by the department to mitigate security threats when there is work-related content removed from the office and is therefore in the employees' possession for remote working. The general response was that currently, information when working remotely is not adequately protected.

The respondent **(R6)** responded that

"I lock it [my laptop] up in my wardrobe in my bedroom because I do not have a safe for the laptop because it is bigger than my safe".

The respondent **(R1)** suggests

"creating awareness on the MISS policy that guides how to protect data when working remotely".

The respondent **(R8)** stated that

"it is an issue. It is not protected. I could take my laptop and lose it, or someone could crack my password. So that's a threat. I would say everything should be stored in the cloud."

The respondent **(R9)** shared the perception that

"I know that when people leave the workplace and have got kids at home, and you can find that the very same laptop for work [X to E] is a resource for the kid [X to E]. When employees are back at home with their laptops, it becomes a play tool for the kids."

"I feel that[X to E] one: we don't save data where it is easily accessible but rather in a secure place; two: ensure the password is kept a secret; three laptops which is a government working tool is solely used for work purposes and nothing else. I should not lend it my [partner] or my kid. So that is how I protect my data when it is my possession outside work."

The respondents shared how they protect data (from theft and unauthorised access) when it is in their possession.

Respondent **(R8)** was concerned that,

"It is an issue. It is not protected; I could take my laptop home and lose it, and someone could crack my password and stuff. So that is a threat. Ideally, I would say everything should be stored in the cloud. That would really make sense".

Another respondent **(R11)** admitted to trusting that no one tampers with the password

"*I rely on the fact that I've got a password, but that password again can be hacked, so it is not really protected*" .

Drawn from the responses from both departments (D1 and D2) similar problem of not observing security protocols during remote working is found in both Eastern Cape Provincial Departments.

Based on the responses from respondents and literature to prepare for the ISA programme, there needs to be a section for remote work in the ISP that states how employees use their devices when not in the office. Secondly, the Eastern Cape provincial Departments should have a risk management policy that sets out how the department and its employees will identify and control the risks due to remote working especially working from home.

6.2.4.3. Theme 3: Understanding employees' perceptions about information security (EP)

The focus of this theme is how employees perceive information security in their Eastern Cape Provincial Departments. Bemis (2015) states that implementation of the ISA programme allows

for an opportunity to explain to employees any concepts in the ISP, which may not clearly explain how they must comply concerning information security. In other words, the perceived self–efficacy, the sense that the employee feels that they can behave expectedly, influences how the employee behaves. Employees' perceived self-efficacy leads to better acceptance of the suggested behaviour during the ISA programme.

Understanding employees' perceptions about the information security theme will be analysed in terms of the respondents' responses and be grouped according to the sub-categories identified (*cf.* Table 9).

6.2.4.3.1. Compliance with Information Security Policies (ISPs)

In the Eastern Cape Provincial Departments, employees must comply with ISPs to reduce information security incidents (Bauer, Bernroider, & Chudzikowski, 2017). The employees should feel confident that they can abide by ISPs as required (Menard, Bott, & Crossler, 2017).

The majority of the respondents were confident that employees could comply with their Eastern Cape Provincial Department's ISP requirements if they were made aware of the policy.

The respondent **(R7)** suggested that,

> *"if the levels of awareness can be raised such that employees can be curious of wanting to read the policies and procedures*."

The respondent **(R2)** also added that we need *"continuous security awareness until it becomes part of you."*

Respondent **(R3)** stated that it is "*the management of the department [who] is supposed to make awareness [known] to people".*

Based on the responses from the respondents in both D1 and D2 and from the literature - to prepare an ISA programme, the ISP should be made known to all employees in a provincial department through information security awareness sessions.

6.2.4.3.2. Simplification of Information Security Policies (ISPs) and Procedures

Bulguru et al. (2010) state that an ISA programme significantly affects employee confidence to comply with ISPs. Consequently, employees who understand the benefit and value of information security in their Eastern Cape Provincial Department have a higher sense of ISA, which leads to better compliance with ISPs. However, as previously explained (*cf.* section 3.6), it is advisable to simplify policies and procedures for employees to ensure that they are understood and accessible (Bemis, 2015). Simplifying ISPs should form part of the ongoing design of ISA messages because the main aim is to raise employee awareness and change their information security behaviour.

The respondent **(R3)** had this view that

> *"policy is supposed to talk to people in terms of how do they conduct themselves in terms of security."*

There were no significant differences in opinions of the respondents on this category in both D1 and D2, and some of their utterances have been used elsewhere in this theme and repeated here.

Based on the respondents' responses and the literature, the employees feel that the ISPs should be written in a simple, easily understood and accessible for compliance. To prepare the ISA programme, the Eastern Cape Provincial Departments need to provide ISPs on departmental websites and other data repositories of the Eastern Cape Provincial departments.

6.2.4.3.3. Reduction of chances of information security threats

The Minimum Information Security Standards (MISS) provide guidelines for the minimum information security measures that any institution must put in place for sensitive or classified information to protect national security. Government employees working with government information resources must know MISS document very well (Michalsons, 2017).

Regarding information security threats, the respondent **(R1)** suggested that the

> *"Minimum Information security standards (MISS) is a straightforward document, but it's quite concise in how everybody can protect information. It tells you where you should leave your laptop, which hotspots you should join. If everybody reads that document, read the policies and use the useful tools that are given to you by the bigger organisations like SSA, SITA […], you will understand what you can do."*

The respondent **(R2)** suggested that,

"all government employees should read the MISS document thoroughly to know how to protect information."

The respondent **(R1)** suggested that the MISS document be sent to all employees by email and utilise the National School of Government to enforce this standard.

"I think if the government does that, we will kill 80% of our information security problems because that document is a real concise document".

A shortcoming of the MISS document can be its currency. Still, staff need to be continuously encouraged to follow good security practices such as password management to reduce threats.

Another respondent **(R3)** added the password reset as another measure that can be used to reduce threats and stated that

"*in my department, you need to change your password after a month. Which is a good thing because once you have the same password for almost a year, chances of it being sniffed are very high*."

However, another respondent **(R1)** had an opposing opinion on the password reset on the basis that resetting the password is outdated and does not serve the purpose of reducing security threats

"*[…] we must move from password changing. Users should get a password and stick with it as long as it's never breached, make it strong that you never have to change it".*

There were conflicting views amongst the respondents on the efficacy of password management by people, which demonstrates the differing perceptions of staff regarding information security controls and managing threats.

Based on the responses from the respondents and the literature, to prepare the ISA programme, top management should make it mandatory for employees to attend a short course on the MISS document at the National School of Government and make it available on the provincial websites. However, this action should not be considered the extent of ISA.

6.2.4.3.4. Reinforcement of good information security behaviour

To change the information security behaviour of employees, an organisation should empower its employees with not just information about risks and expected security behaviour, but employees should understand and apply those recommendations (self-efficacy) (Bada & Sasse, 2019).

Secondly, employees must be motivated and willing to do so (perceived response efficacy). Employees must change their attitudes and intentions *(Perceived Response Cost)* as suggested by the Protection Motivation Theory. The literature, however, warns against the usage of excessive sanctions (*cf.* section 2.4).

For effective implementation of the ISA programme for employees, the programme should not be exercised by imposing excessive fear (sanctions) on simple, consistent rules of behaviour that are easily followed (Bada and Sasse, 2019).

The respondents in the interview sessions provided some insights on promoting good information security behaviour.

Respondent **(R11)** said, *"I think accountability and consequent management*."

Respondent **(R1)** suggested the following:

> *"I think definitely education, awareness and then visible sanction for non-compliance.*"

Respondent **(R8)** advised that the actions need to be continuous,

> *"Communication, communication, enforce it. Send it out. Warn the people. You know it must be in their faces all the time. Not once a year, but be there every time, prompts on the laptops".*

Finally, the respondent **(R5)**

> *"Continuous awareness sessions allow people to understand security risks and threats, and the consequences of non-compliance behaviour".*

The *Code of Conduct* document had also been raised by respondent **(R1)** to integrate ISA into the daily operations of the staff.

To prepare the ISA programme in a provincial government setting, there need to be scheduled easy-to-follow ISA sessions held frequently. Additionally, the sanctions for non-compliance should be incorporated into the already existing government Code of Conduct document.

6.2.4.3.5. Sanctions for Non-compliance of ISPs

As the Protection Motivation Theory explains (*cf.* section 2.4.2), what motivates employees to protect information assets comes from a perceived threat of complying or not complying and a need to avoid a potentially negative consequence. Perceived threat severity, therefore, is the employee's opinion of how serious that particular threat is.

The respondents shared their perceptions on the sanctions that are in place in their Eastern Cape Provincial Departments concerning ISPs being violated and their opinion on the likelihood of a change of employees' security behaviour if those sanctions are severe.

The respondent **(R7)** stated that,

> *"I've never heard of anybody losing their jobs in my department because of information security".*

The respondent **(R8)** also had a similar opinion by stating that,

> *"no, no, I'm not aware of anybody I know in all the time I've been here. I've never had an instance when this has happened."*

another perception of the respondent **(R7)** was that

> "*to a certain extent, you also need to have punitive measures, what are the consequences of not abiding by the rules [X to E]".*

Based on the respondents' responses from both D1 and D2 and the literature, the employees feel that sanctions should be imposed on those employees who violate information security policies. To prepare the ISA programme, ISPs should have a section informing employees of the severity of sanctions for non-compliance to ISPs.

6.2.4.4. Theme 4: Conducting Information Security Awareness and Training (SA)

Employee ISA positively affects information security compliance in the Eastern Cape Provincial Department (Alkabani, Deng, & Kam, 2018). To mitigate the human risk, an organisation should change employees' behaviour and how employees behave, and the Eastern Cape Provincial Department requires a mature awareness program (SANS Security Awareness Report, 2019). Without employee information security awareness, the organisation can have security breaches irrespective of putting technical and physical security measures in place (Wahyudiwan, Sucahyo,

& Gandhi, 2017). Aldawood and Skinner (2019) agree with the statement and assert that information security awareness is the only known defence for attacks such as social engineering and warn that unless employees in the Eastern Cape Provincial Departments are aware of these threats posed by social engineering, they are vulnerable to threats and will put the Eastern Cape Provincial Department's information assets at risk. For an ISA programme to succeed, it should be conducted on an ongoing basis, and not just a yearly activity, but should strive to maintain security awareness every day (Stefaniuk, 2020). The theme will be analysed in terms of the respondents' responses and be grouped according to the categories identified (*cf.* Table 9).

6.2.4.4.1. Customised information security awareness and training modules

The Eastern Cape Provincial Department should select the right employees for the training based on their needs. Amjad, Naeem, and Zaffar (2016) suggest that adult trainees need to be actively engaged and the material immediately valuable and relevant to their day to day life to be effective. The Eastern Cape Provincial Department, therefore, has to find out what challenges the target audience is experiencing, and these challenges must find expression in the ISA programme (Arash & Zarina, 2017). Additionally, it is essential to ensure that during ISA training, the facilitator relates the course content to the specific environment under which the Eastern Cape Provincial Department operates in terms of its mission and culture requirements (NIST Special Publication 800-16, 2018).

The respondents could not articulate what customisation needed to occur, and this was considered a shortcoming arising from a lack of understanding of the nature of an ISA programme. Although, Respondent **(R1)** did say that it is necessary "*to ensure relevant people attend the training"***.**

6.2.4.4.2. Listing of relevant information security awareness and training topics

The initial step critical for the ISA training programme is to conduct a needs assessment and establish employees' level of information security literacy (Nieles et al., 2017). It is also crucial to ensure the topics for the ISA programme are designed for the trainees' needs and not offer generic training that simulates classroom lectures with no practical application (Wahyudiwan et al., 2017).

The respondents raised various topics (and buzz words, which are omitted) that are information security-related, which they felt need to be included in an ISA programme: password management and security, email use, information about phishing and scams, physical access requirements to information assets, how to have a clean desk policy, the sanctions for ISP infringements, cloud security requirements, and undertaking backups.

To prepare an ISA programme in an Eastern Cape Provincial Department, the facilitator of the ISA sessions needs to determine the topics for inclusion in training. These can either be sourced directly from staff or utilised from other online sources. However, all the topics must be contextualised for the staff.

The following section will discuss the proposed framework for preparing an information security awareness and training program for government employees in the Eastern Cape Province in South Africa.

6.3. Presentation of the framework - preparing an Information Security Awareness Program

This study used a case study design to investigate the information security phenomenon in the Eastern Cape provincial government to develop a framework for preparing an information security awareness program. The data analysis discussed in the previous section detailed the findings from the study. The output of this study is in the form of a framework derived from the literature and primary data collected. A framework assists a researcher in identifying and constructing their viewpoint of the phenomenon being investigated (Adom, Hussein, & Agyem, 2018). The framework is a proposed answer to the problem under investigation. It is a proposal of the researcher's solution to the research problem they have defined (Adom et al., 2018).

The four critical components of the framework (Figure 10) are explained; after that, we discuss how the framework addresses the research question asked: ***How should the Eastern Cape provincial government prepare an information security awareness programme to foster information security amongst employees in government departments?*** The framework has also been developed to accomplish the research objectives of this research project.

The framework is presented as a set of questions for completion when undertaking an ISA programme. The questions are completed by selecting the status of each category. The status colours are **Red** representing 'No'; **Yellow/Amber** for 'Partial'; and **Green** representing 'Yes'. The red status means that the department is not completing the essential category elements for preparing the ISA and training program. Commencing with some items being on red status means that the information security awareness and training program runs a high risk of being unsuccessful. The amber status means that the category element defined on the framework exists but is not yet fully realised. Therefore, the Eastern Cape Provincial Department's goal is to take such action necessary to change the status to green. The green status means that the category element exists and or is in full operation. The intention is that the framework works as a matrix that gives those responsible for preparing the ISA programme a view of where there are issues that need to be addressed to improve the likelihood of the successful rollout of the programme.

The four key components of the framework are **[Step 01]** Identifying Organisational Information Security Culture, **[Step 02]** Identifying Information Security Risks and Threats, **[Step 03]** Understanding Employee Perceptions about Information Security, and **[Step 04]** Conducting Information Security Awareness and Training. Each of these steps as they apply to the framework will be discussed further.

[Step 01] Identifying Organisational Information Security Culture

The leadership of an organisation that expresses its expectations entrenches them gradually and continually in its vision, mission, goals, structures, and employees' activities (Nel & Drevin, 2019). Therefore fostering organisational ISC is crucial for effective ISC. Most importantly, the Eastern Cape Provincial Departments should ensure that security culture is established within the provincial departmental (organisational) culture and periodically assess their security culture. After that, the activities performed in an organisation are consistent with a good ISC (Amankwa, Loock, & Kritzinger, 2018; Palega & Knapinsski, 2019).

Preparation Step	Category	Question	Status		
Step: 01 Identifying Organisational Information Security	1.1. Commitment of Top Management	Is there a commitment from top management?			
	1.2. Existence of Information Security Strategy	Does an Information Security Strategy exist?			
	1.3. Allocating of Information Security Awareness and Training Funding	Is funding allocated to Information Security Awareness and Training?			
	1.4. Communicating of Continuity Plans	Are Continuity Plans communicated to staff?			
	1.5. Enforcement of Information Security Accountability	Is Information Security Accountability enforced?			
Step: 02 Identifying Information Security Risks and Threats	2.1.Incorporation of ISPs into the New Hire Process	Are ISPs incorporated into the New Hire Process			
	2.2. Access to ISPs	Are ISPS accessible?			
	2.3. Classification of Organisational Information *(Top Secret, Secret and Confidential)*	Is the Organisational Information classified *(Top Secret, Secret and Confidential)?*			
	2.4. Update Employees on new incidents	Are employees' updated on new incidents regularly?			
	2.5. Notification of recent information security breaches and threats	Are employees notified of recent information security breaches and threats?			
	2.6. Establishing Information Security Protocols for Remote Working	Are Information Security Protocols for Remote Working established?			
Step: 03 Understanding Employee Perceptions about Information Security	3.1. Compliance with Information Security Policies	Do employees comply with Information Security Policies?			
	3.2. Simplification of Information Security Policies and Procedures	Are Information Security Policies and Procedures simplified?			
	3.3. Reduction of Chances of Information Security Threats	Are there any measures to reduce the chances of Information Security threats?			
	3.4. Reinforcement of Good Information Security Behaviour	Is good Information Security Behaviour reinforced?			
	3.5. Sanctions for Non-compliance to ISPs	Are there any sanctions for Non-compliance to ISPs?			
Step: 04 Conducting Information Security Awareness and Training	4.1. Customised Information Security Awareness and Training Modules	Are information security awareness and training modules customised?			
	4.2. Listing of relevant Information Security Awareness and Training Topics	Are relevant information security awareness and training topics listed based on the training needs?			

Figure 12. : Proposed Framework for Preparing an Information Security Awareness and Training Programme

Hence the management of the Eastern Cape Provincial Department must establish a security culture within the organisational culture (Karlsson, Denk, & Åström, 2018). It is the responsibility of the top management to create an environment of learning the values of the Eastern Cape Provincial Department for its employees and help them be capable of complying with ISPs to improve compliance (Shouran, 2019; Thomson & Van Niekerk, 2011).

A brief description of each category is provided of the framework (Figure 12), which should ideally present a green (optimal) outcome based on the colour coding of the framework.

Category 1.1. Commitment of the Top management

Visible participation, support and involvement of the top management are required to ensure information security policy compliance and information security awareness and training is taken seriously.

Category 1.2. Existence of Information Security Strategy

Development and implementation of information security strategy where departments can draw clarity and consistency should be developed to instil ISC.

Category 1.3. Allocating of Information Security Awareness and Training Funding

Providing an information security budget is linked to having an information security strategy in place, as suggested in Chapter 3 (*cf.* section 3.6). The information security budget dedicated to funding all information security resources and information security awareness activities should be allocated annually by the Eastern Cape Provincial Department.

Category 1.4. Communicating of Continuity plans

Assessing the current ISC with respect to disaster recovery, communicating business continuity plans to employees, and easy access to these plans when needed is critical.

Category 1.5. Enforcement of Information Security Accountability

Incorporation of employee ISA and training in the Code of Conduct document with clearly defined sanctions for noncompliance is required to enhance information security accountability.

[Step 02] Identifying Organisational Information Security Risks and Threats

Information security risks are identified when possible security threats have emerged which can exploit vulnerabilities of information assets and therefore can be a reason for harming an organization (Shamala et al. (2017). The Eastern Cape Provincial Departments has therefore identified the following as threats that can exploit vulnerabilities of information, namely: Incorporation of ISP into the new hire process; Access to ISPs and Minimum Information Security Standards (MISS); Classification of organisational information (Top secret, Secret and Confidential); Update employees on new incidents; Update employees on new incidents; Notification of recent information security breaches and threats; Establishing Security Protocols for Remote Working. Each of these Organisational Information Security Risks and Threats will be discussed briefly below.

Category 2.1. Incorporation of ISP into the new hire process

Information security requirements should always be included in the processes of newly appointed employees to ensure that ISA and training objectives are marketed without relying on each unit of the Eastern Cape Provincial Department to conduct ISA.

Category 2.2. Access to ISPs and Minimum Information Security Standards (MISS)

Easy access through various awareness and training delivery methods (cf. section 3.3) to ISPs, awareness sessions for ISPs and the MISS document should be facilitated to ensure there is awareness and employees' compliance to ISPs.

Category 2.3. Classification of organisational information (Top secret, Secret and Confidential)

Development and implementation of a clean desk policy to ensure that classified information is safeguarded are required.

Category 2.4. Update employees on new incidents

Provision of information security briefs and educating employees on any recent incidents and how to deal with this incident to prevent reoccurrence is required.

Category 2.5. Notification of recent information security breaches and threats

Employee notification systems on the recent information security breaches and threats to train employees on how to detect security threats should be put in place.

Category 2.6. Establishing Security Protocols for Remote Working

Remote work security risk management policy to set out how the department and its employees will identify and control risks due to remote working, especially working from home, is required.

[Step 03] Understanding Employee Perceptions about Information Security

It Is the responsibility of the top management to understand the perceptions of the employees about information security to convince them to comply with ISPs. The employees should thererefore be made to feel confident that they can comply with ISPs as required. The top management can facilitate the understanding of Information securty by communicating security policies to increase their confidence to comply with the requirements of their department's information security policy. The policies are recommended to be updated to align with rapidly changing technology to meet the department's needs. The staff should be workshopped on the updates of the revised policies, and these must be distributed to all staff. On the other hand, security awareness significantly affects employees' confidence in complying with security policies with regards to the benefit of compliance and the cost of non-compliance.

What the employees perceive as a threat to complying with information security policies they avoid and similarly employees will also avoid the negative consequences of not complying (Menard, Bott, & Crossler, 2017). Consequently, employees who know the benefit and value of information security in their provincial departments have better ISA, which leads to good compliance with ISPs. It is advisable to simplify policies and procedures for employees to ensure that they are understood and accessible to employees for them to apply the policies (Bemis, 2015). Simplifying security policies should be manifested again in designing security awareness and training messages because the main aim is to change employees' security behaviour.

Category 3.1. Compliance with Information Security Policies

Employee motivation to ISP compliance through increasing their confidence in understanding ISPs is important and should be done by conducting frequent ISA sessions

Category 3.2. Simplification of information security policies and procedures

Designing ISA and training messages in a simplified manner with the aim of changing employee compliance behaviour is required.

Category 3.3. Reduction of chances of information security threats

Mandatory attendance of a short course on the MISS document at the National School of Government and easy access of the MISS on all information security delivery methods (including departmental website) is required.

Category 3.4. Reinforcement of good information security behaviour

Conducting easy-to-follow ISA sessions which aim to increase knowledge and confidence, which motivates employees to comply with ISPis critical.

Category 3.5. Sanctions for non-compliance of ISPs

Incorporating sanctions for non-compliance to ISP on the already existing Code of Conduct for Government employees is required. The literature, however, warns against excessive sanctions, as discussed in Chapter 2 (*cf.* section 2.4).

[Step 04] Conducting Information Security Awareness and Training

Without employee information security awareness, the organisation can have security breaches irrespective of putting technical and physical security measures in place (Wahyudiwan, Sucahyo, & Gandhi, 2017). Aldawood and Skinner (2019) agree with the statement and assert that information security awareness is the only known defence for attacks such as social engineering and warn that unless employees in the organisation are aware of these threats posed by social engineering, they are vulnerable to threats and will put the Eastern Cape Provincial Department's information assets at risk.

Category 4.1. Customised information security awareness and training module

For a specific ISA and training, selecting suitable employees for the training based on their security needs and background is required.

Category 4.2. Listing of relevant information security awareness and training topics

Tailoring the course content to the specific environment and followed by listing relevant security topics is important to offer content-specific topics, and to avoid ineffective generic security training is important.

6.4. Conclusion

This chapter gave discussed the research findings and how they were explored and incorporated to prepare an initial framework for the Eastern Cape Provincial Departments' ISC awareness programme. This framework was produced by logically analysing primary data. The framework's constructs were derived from the results obtained from this study's interview transcripts and literature review. To be able to use the data, it was coded. The codes were generated from the pre-defined key areas of focus of the study taken from literature and the two theories that were used to ground this research project which discusses how the organisational culture can facilitate the ISC, the importance of security compliance, accountability, employee perceptions, and security awareness and training in changing employee behaviour towards reducing security risk and threats. These codes were plotted against a semi-structured interview guide.

The respondents' (R1, R2, R3, R4, R5, R6, R7, R8, R9, R10 and R11) responses from the two provincial departments (D1, D2) were all part of the analysis discussion. Each theme was discussed, and then respondent responses were included to provide evidence from the government employees on the given theme focus. The findings then were used to determine the outcome of this research project which is the framework for preparing an ISA and training programme. The study's outcome was achieved by condensing the themes that emerged in both the primary and secondary data. The framework, which includes questions and a colour code ranking, make it quickly operational. Each category in the framework was briefly explained so that the intended meaning was known.

CHAPTER SEVEN: CONCLUSION

7.1. Overview
7.2. Theoretical Focus and Literature
7.3. Objectives of the Study
7.4. Research Methodology
7.5. Discussion
7.6. Future Research
7.7. Concluding Remark

7.1. Overview

Chapter Six discussed the findings and recommendations detailing how the data analysis process was followed to derive the proposed *Framework for Preparing an Information Security Awareness and Training Programme*. Primary data and secondary data were used in the process of developing the framework. The primary data was obtained from Eastern Cape Provincial Departments' employees using an interview guide to conduct the semi-structured interviews, which assisted in concluding with the findings of this research study.

To describe how the study arrived at the proposed framework, a summary and conclusion of this research are made in this chapter. *Firstly,* this chapter discusses how the literature was conducted in the study, with direct references to the underpinning theories used as the primary focus for this research project: the Organisational Culture Theory (OCT) and the Protection Motivation Theory (PMT). *Secondly*, this chapter restates the research problem that led to the main research question and sub-question and discusses the research sub-questions in each chapter. *Thirdly*, the next chapter to follow was the Research Methodology chapter, detailing the process of collecting and analysing data. Fourthly, the limitations of this study are presented. *Finally*, this study delivers concluding remarks.

7.2. Theoretical Focus and the Literature

The main focus of the literature review conducted in this study was on ISA, training, and ISC. Organisational culture was discussed as part of establishing an ISC in the provincial departments. These two constructs are information security risks and threats and employees' motivation to comply with ISPs. They are concerned with how employees' behaviour can be influenced to foster a good ISC. ISA and training are linked to security risks and threats, which seeks to mitigate these security risks and threats. These constructs were discussed concerning the relevant literature on how information security awareness can assist in instilling an ISC within government departments. A summary of the constructs will be presented concerning the underlying theoretical focus, which is key in the discussion of this study.

The (OCT) and (PMT) were presented with core tenets based on this research study. Each of the theories that have been used (*cf.* section 1.6) are discussed within the context of the relevant chapter. Chapter Two focused on **security risks and threats**, and Chapter Three on **information security awareness and training** and Chapter Four on **organisational information security culture**

Information security awareness is the common theme found across the research project because it is the underlying phenomenon, which improves information security policy compliance and reduces security risks and threats. The reason is that the Eastern Cape Provincial Department can use information security awareness programmes as a vehicle to build an ISC in a department.

Organisations conduct information security awareness and training to ensure employees know information security policies and procedures (Bauer, Beroider, & Chudzikowski, 2017). Information security awareness leads to better security behaviour and compliance to ISPs (Bauer, Beroider, & Chudzikowski, 2017). When employees are aware that ISPs exist in the Eastern Cape Provincial Department, and their perception of these policies is that they are simple to follow, employees will comply with them. This is the underlying principle of the PMT, self-efficacy to comply with ISPs.

Therefore, the organisation must make information security a routine activity of every employee performing their job (Van Niekerk & Von Solms, 2010). Top management buy-in and support then become critical by encouraging information security on the daily activities of its employees. This is the underlying principle of Organisational Culture Theory (OCT).

The most significant information security risk that is directed to organisations is posed by its employees (Giandomenico & De Groot, 2018). Employee compliance with ISPs reduces security risks and threats because ISPs specify how employees should behave. Critical to ISP compliance motivates employees to comply and thereby protect the information assets of the department. This is the underlying principle of Protection Motivation Theory (PMT) regarding threat severity or perceived self-efficacy. Threat severity means that what motivates employees to protect information assets is based on the perceived threat of compliance or non-compliance and, therefore, a need to avoid a potentially negative consequence. For example, an Eastern Cape Provincial Department might want to discipline any employee who violates information security policies or might decide to terminate the employment of all employees who repetitively violate ISPs. Perceived self-efficacy is the level of confidence in one's ability to undertake the recommended preventive behaviour.

Linked to perceived self–efficacy or employee's perception that ISPs are simplified is the provision of information security awareness and training by the Eastern Cape Provincial Department. Security awareness and training should be designed so that employees are persuaded to change their security behaviour by pointing out the advantages of complying with ISPs. The success of an ISA and training programme in the department depends on the benefits of the

programme being explained to the department's top management for the necessary buy-in, support, and allocation of funds to the programme. Hence, ISC must be part of the organisational culture because it is one of its functions, as stated in the Organisational Culture Theory. By building organisational information culture, an organisation can motivate employees to protect information assets against numerous security threats (Al Hogail A. , Design and validation of information security culture framework, 2015).

7.3. Objectives of the Study

The primary objective of this research project was the development of a framework to prepare Information Security Awareness and Training Programme in the context of the Eastern Cape Provincial Government Departments. The proposed framework can establish an ISC within the Eastern Cape Provincial Government Departments, which will mitigate security risks and threats.

The framework was derived by investigating the following research question:

How should the Eastern Cape Provincial Government prepare an information security awareness programme to foster an information security culture amongst employees in government departments?

The main research question was investigated by addressing three sub-questions, which were discussed in the relevant chapters as indicated below:

Q1: How do employees contribute to information security risks and threats?

Chapter Two discussed an insight on how employees can mitigate security risks and threats. This is explained by examining the nature of information security. After that, the key areas of information security regulatory compliance and the significance of information security audits were discussed. After that, a discussion was undertaken on the importance of information assets, identifying risk, and putting controls to mitigate those risks. The main underlying theoretical premise of what motivates employees to comply with ISPs was the Protection Motivation Theory (PMT). The underlying premise of PMT is that employees should be made aware that ISPs exist in the Eastern Cape Provincial Department. Employees should be made to read them and be confident that they can implement the policy to safeguard the organisation's information assets.

Q2: What are the main factors that influence information security awareness among employees?

Chapter Three provided a discussion of the nature of information security awareness and detailed how the ISA training programme structure should be done. The various steps in the preparation of security awareness and training programmes were elaborated upon. The ISA programme in developed countries was explored to understand the application of ISA in these countries and the lessons learned by these countries. After that, ISA programmes in developing countries was also explored. The aim was to understand the application of ISA programmes by developing countries, the challenges experienced, and the lessons learnt. After that, a discussion on how an ISA programme can enable an Eastern Cape Provincial Department to build an ISC.

Q3: What are the requirements to consider when fostering an information security culture in provincial government?

Chapter Four discussed the role of organisational culture as an enabler for ISC establishment. The factors that are required to foster ISC were then discussed.

The discussion of the differences between organisational culture and ISC was expanded because a successful establishment of ISC cannot be assessed in isolation but within the organisational culture. This was explained by focusing on how the Eastern Cape Provincial Departments' management should establish the ISC within the organisational culture to motivate the employee to behave to safeguard the information assets. Later on, the chapter concludes with a discussion of how the assessment of the current ISC can enable the Eastern Cape Provincial Departments to know the level at which the Eastern Cape Provincial Departments is protecting security assets to reduce security risks and threats. Additionally, the results of the assessment enable the Eastern Cape Provincial Departments to identify areas of improvement.

The importance of ISC in influencing the behaviour of employees and motivating employees to comply with security policies was also elaborated upon. Additionally, the role played by the Eastern Cape Provincial Departments 's top management was emphasised as the management's responsibility is to create an environment for employees to learn the organisation's values and, therefore, would be instrumental in assisting employees in complying with information security policies. ISC can, therefore, be cultivated where employees have a good perception and knowledge about security policies. Thus, information security policies play a pivotal role in influencing the ISC and is key in establishing shared values and beliefs.

Additionally, the chapter concludes that awareness, training, and education improve employees' understanding of security risks and threats to information assets and ways to control them. The

Eastern Cape Provincial Departments should conduct security awareness through top management's support to investigate the effectiveness of organisational culture on ISC.

From a theoretical perspective, this chapter detailed some issues surrounding the tenets of the Organisational Culture Theory such as employees' patterns of behaviour or awareness courses which is the principle of Organisational Culture Theory (*Artifacts*); security strategies, the vision of the Eastern Cape Provincial Departments, which is the principle of Organisational Culture Theory *(Espoused values)*; Shared security values, habitual and unconscious security behaviours which assist in ensuring compliance which is the Principle of organisational theory (*Shared tacit assumptions*). The Protection Motivation Theory was implied by considering that when there is an organisational culture that encapsulates ISC, the management may see improvement in employees' perception of understanding security policies. The Eastern Cape Provincial Departments need to understand that employee compliance should not be forced to comply but result from individual self-motivation or choice. This is the fundamental principle of perceived self-efficacy, which stresses confidence in one's ability to undertake the recommended preventive behaviour.

7.4. Research Methodology

Chapter Five gives a detail of the research methods that were followed. An explanation was given on what a paradigm is, and justification for selecting the interpretivism paradigm to be used in this study was given because of the subjective nature of the phenomenon being investigated: information security awareness and training. Because interpretivism is chosen as the appropriate paradigm, a qualitative research design was justified. Using qualitative research allowed semi-structured interviews to be selected, which were informed by the interview guide. The interview guide was generated out of the literature review conducted. The questions of the interview guide were then sorted into themes (topics) so that they became easy to interpret when analysing the data.

Semi-structured online interviews were conducted using Microsoft Teams as it was during the COVID 19 pandemic. The interviews were conducted with 12 respondents from two departments in the Eastern Cape provincial government. In the first stage, respondents from department 1 (D1) (IT managers and employees) were interviewed, and in the second stage, respondents from department 2 (D2) were interviewed. The questions that the researcher prepared and provided were derived from the literature as well as the objectives of the study to collect only the necessary information from the participants of the interview.

The research project utilised a case study to address how a provincial government needs to focus on employees' ISA and training to improve ISC to realise unqualified audits on information security. The prepared questions were asked from the respondents in the two departments as a Case Study of the provincial government. The following section will provide a discussion of the study conducted and how the study's primary objective was achieved.

7.5. Discussion

A literature review on the secondary data was conducted for this research project to understand the research problem, i.e. how the Eastern Cape Provincial Government needs to focus on employees' information security awareness to improve ISC and realise unqualified government audits for information security. The literature review considered the discussion on information security awareness and training. The purpose of implementing ISA and training is to make employees understand and be aware of security risks and threats to information assets and control thereof, to apply and comply with.

The literature also identified that if employees comply with ISPs, security threats are minimised. Also, key findings from the literature were what motivates the employees to comply, which was found to be sanctioned for non-compliance and confidence that they understand what they are supposed to comply with. Critical for employees to enable them to understand is that ISPs should be simple and easily understood. Also, employees should get the necessary ISA and training and be motivated to comply with ISPs. If there is a lack of support for ISA and training, employees could be reluctant to demonstrate an expected change of information security behaviour.

The literature further identified that by building an ISC, the provincial department could motivate employees to protect information assets against security threats. Information security awareness and training programmes can be a powerful strategy to enhance employees' compliance and assist in securing the department's information assets. The ISA and training can also assist in forming up an organisational ISC that appreciates employees' behaviour that complies with security policies, thereby mitigating security risks and reducing security threats.

The research process moved from literature review to collecting data, analysing data, and interpreting the Information Security Awareness and Training Framework, which highlighted the need for frequent and continuous information security awareness workshops, customising awareness and training modules, and listing security and awareness topics. It is believed that the aim of this research project has been achieved, i.e. the preparation of an information security

awareness and training programme for the provincial government to raise awareness of users and to change employee behaviour towards information security.

7.6. Future Research

This research project focused on the preparation of concepts for information security awareness and training. This framework should also be tested in establishing ISC in the government context, be it local, provincial, or national government.

This research project focused only on internal users (employees) of the department and how their security behaviour affected information assets of the department. Further research should be conducted on external users (visitors as well as suppliers to the department).

7.7. Concluding Remarks

The research project provides an understanding of the processes and activities performed by employees to address information security risks and threats and the factors needed to prepare ISA and training programmes for Eastern Cape Provincial Government employees. The significance of this study as per the constructs of ISA and training has been shown in a diagram. It can challenge thinking of how ISA can be prepared for not only provincial government but for state-owned entities or local government as well. The study discovered solutions to ISP compliance at the organisational level and at the individual level. At an organisational level, organisational ISC ensures that there is buy-in and support from executive management, the information security strategy exists, continuity processes exist and are communicated to employees. At an individual level, they are motivating employees to comply with ISPs, by ensuring that they understand the ISPs and implications of noncompliance (sanctions). The research project also proposes that to ensure compliance at the organisational level and individual level, the department should conduct ISA.

REFERENCES

Abawajy, J. (2018). User preference of cyber security awareness delivery methods, Behaviour &. *Behaviour & Information Technology, 33*(3), 237-248.

Adom, D., Hussein, E., & Agyem, J. (2018). Theoretical and conceptual framework: mandatory ingredients of a quality research. *International Journal of Scientific Research, 7*(1).

Al Hogail, A. (2015). Cultivating and Assessing an Organisational Information Security Culture; an Empirical Study. *International Journal of Security and its Applications, 9*(7), 163-178.

Al Hogail, A., & Mirza, A. (2014). Information Security culture; a definition and a literature. *IEEE World Congress on Computer Applications and Information Systems*, (pp. 1-7). Saudi Arabia.

Al Hogail, A., & Mirza, A. (2017). Information security culture: A definition and a literature review. *Computer Applications and Information Systems*, 1-7.

Alavi, R., & Islam, S. (2016). An information security risk-driven investment model for analysing human factors. *Information and Computer Security, 24*(2), 205-227.

Aldawood, H., & Skinner, G. (2019). Challenges of Implementing Training and Awareness Programs targeting cyber security social engineering. *Cybersecurity and cyberforensics Conference (CCC)*, 1-7.

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture: A Behaviour Compliance Conceptual Framework. *8th Australasian Information Security Conference*, *105*, pp. 47-55. Brisbane.

AlKabani, A., Deng, H., & Kam, B. (2015). Organisational security culture and information security compliance for e-government development: the moderating effect of social pressure. *Pacis2015.* Melbourne.

Alkabani, A., Deng, H., & Kam, B. (2018). Investigating the Role of Socio-organisational Factors in the Information Security Compliance in Organisations. *Australasian Conference on Information Systems* (pp. 1-11). Adeilade, Australia: RMIT University.

Alnatheer, M., & Nelson, K. (2009). A proposed framework for understanding information security culture and practices in the Saudi context. *Proceedings of the 7th Australian Information security management conference*, 1-17.

Aloitabi, M., Furnell, S., & Clarke, N. (2016). Information Security Policies: a review of challenges and influencing factors. *The 11th International Conference for Internet Technology and Secured Transactions (ICITST-2016)* (pp. 352-358). Plymouth: IEEE.

Alshaikh, M., Maynard, S., Ahmad, A., & Chang, S. (2018). An exploratory study of current information security training and awareness practices in organisations. *Proceedings of the 51st Hawaii International Conference on System Sciences*, (pp. 5085-5094). Melbourne.

Alshaikh, M., Maynard, S., Ahmad, A., & Chang, S. (2018). Information Security in Agile Software Development Projects: a Critical Success factor Perspective. *Proceedings of the 51st Hawaii International Conference on System Sciences*, 5058-5094.

Amankwa, E., Loock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. *Information and Computer Security, 26*(4), 420-436.

Amjad, H., Naeem, U., & Zaffar, M. (2016). Improving security awareness in the government sector. Shanghai, China.

Angraini, R., Alias, & Okfalisa. (2019). Information Security Policy Compliance: Systematic Literature Review. *The Fifth Information Systems International Conference 2019* (pp. 1216–1224). Procedia Computer Science.

Arachchilage, N. G., & Love, S. (2016). Security awareness of computer users: A phishing threat avoidance. *Computers in Human Behavior*, 304–312.

Arash, G., & Zarina, S. (2017). A framework for an effective information security awareness program in healthcare . *International Journal of Advanced Computer Science and Applications, 8*(2), 193-205.

Arbanas, K., Spremic, M., & Hrustek, N. (2021). Holistic framework for evaluating and improving information security culture. *Aslib Journal of Information Management, 73*(5), 699-719.

Ashenden, D. (2018). In their own words: employee attitudes towards information security. *Information and Computer Security, 26*(3), 327-337.

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy? *Computers & Security, 39*, 396–405.

Astakhova, L. (2015). Information security: risk related to the cultural capital of personnel (Review). *Sci. Tech. Inf. Process, 42*(2), 41-52.

Astakhova, V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture-Perspective from academia and industry. *Computers & Security, 92*, 1-53.

Bada, M., & Sasse, A. (2019). Cybersecurity Awareness Campaigns: Why do they fail to change behaviour? *Cyber Security Awareness Campaigns*, 1-38.

Bada, M., & Sigurdsson, R. (2020). Cybesecurity for dummies. *AwareGO Special Edition*, 1-50.

Barbie, E., & Mouton, J. (2001). *The practice of social research.* Cape Town: Oxford University Press.

Barreiro, P., & Albandoz, J. (2001). Sampling Techniques: Population and sample. *Management Mathematics for European Schools*, 4-5.

Bauer, S., & Bernroider, E. (2018). From information security awareness to reasoned compliant action: analysing information security policy compliance in a large banking organisation. *ACM SIGMIS Database: the Database for Advances in Information Systems, 48*(3), 44-68.

Bauer, S., Bernroider, E., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers and secrity, 68*, 145-159.

Belanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management, 54*(7), 887-901.

Bemis, B. (2015, May 18). *SecureIT Observations: Why Most Awareness and Training Programs Fail.* Retrieved from SecureITExperts : http://secureitexperts.com/secureit-observations-why-most-awareness-and-training-programs-fail/

Blythe, J., Coventry, L., & Little, L. (2015). Unpacking security policy compliance : The motivators and barriers of employees' security behaviours. *Eleventh Symposium On Usable Privacy and Security*, (pp. 103-122).

Boer, H., & Seydel, E. (1996). *Protection motivation theory.* Buckingham: Open University Press.

Box, D., & Pottas, D. (2013). Improving information security behaviour in healthcare context. *Health and Social Care Information Systems and Technologies, 9*, 1093-1103.

Braun, V., & Clarke, V. (2014). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101.

Breithaupt, J., & Merkow, M. (2014). *Information security principles and practices*. 2ed. Pearson IT Certification: USA

Bryman, A., & Bell, E. (2011). *Business Research Methods.* New York: Oxford University Press.

Bulguru, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Busch, M., Patil, S., Regal, G., Hochleitner, C., & Fröhlich, P. (2015). Persuasive Information Security-A Behavior Change Support System to Help Employees Protect Organizational Information Security. *BCCS@ PERSUASIVE* (pp. 56-66).

Caballero, A. (2017). Security Education, Training, and Awareness. *Computer and Information Security Handbook*, 497- 505. doi:http://dx.doi.org/10.1016/B978-0-12-803843-7.00033-8

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., & Young, S. (2020). Purposive sampling: complex or simple? Research case examples. *Journal of Research in Nursing, 25*(8), 652-661.

Chen, X., Chen, L., & Wu, D. (2017). Factors that influence employees' security policy compliance: An Awareness- Motivation-Capability Perspective. *Journal of Computer Information System*, 1-14.

Chen, X., Wu, D., Chen, L., & Teng, K. (2018). Sanction severity and employees' information security policy compliance: Investigating mmediating, moderating, and control variables. *Information & Management, 55*(8), 1049-1060.

Chen, Y., Ramamurthy, K., & Wen, K. (2015). Impacts of Comprehensive Information Security Programs on Information Security Culture. *Journal of Computer Information Systems, 55*(3), 11-19.

Clubb, A., & Hinkle, J. (2015). Protection motivation theory as a theoretical framework for understanding the use of protective measures. *Criminal Justice Studies*, 1-21.

Committee on National Security Systems. (2001). National Security Telecommunications and Information Systems Security Committee . United States

Connolly, L., & Lang, M. (2018). Information Systems Security: The role of cultural aspects in organisational settings. *Association for Information Systems*, 1-16.

Connoly, L., Lang, M., Gathegi, J., & Tygar, J. (2016). The Efffect of Organisational Culture on Employee Security Behaviour: A Qualitative Study. *Proceedings of the Tenth International Symposium on Human Aspects of Information Security and Assurance, 2016*, (pp. 33-44).

Conolly, L., Lang, M., Gathegi, J., & Tygar, J. (2017). Organisational culture, Procedural countermeasures, and Employee security behaviour: A Qualitative study. *25*(2), 1-24.

Cooper, D., & Schindler, P. (2014). *Business Research Methods.* London: The McGraw-Hill Companies.

Corris, L. (2010). Information Security Governance: Integrating Security Into the Organizational Culture. *Position Paper*, 35-41.

Cotter-Lockard, D. (2016). Edgar Schein's Organizational Culture and Leadership, as seen through the lens of Ken Wilber's AQAL Framework (and the author's eyes). *HOD706 – Social Psychology – In Depth Paper*.

Council, Security Awareness Program Special Interest Group PCI Security Standard. (2014, October). Best Practices in Organisational Security Awareness.

Cram, W., Proudfoot, J., & D'arcy, J. (2017). Organisational information security policies: a review and research framework. *European Journal of Information Systems, 26*(6), 605-641.

Creswell, J. (2014). Research Design. In *Qualitative, Quantitative and Mixed methods* (4 ed., pp. 1-342). SAGE.

Crossler, R., Johnston, A., Lowry, P., Hu, Q., Warkentin, M., & Baskerville, R. (2018). Future directions for behavioural information security research. *Computer security, 32*, 90-101.

Da Veiga, A. (2013). An information security training and awareness approach (ISTAAP) to instil an information security-positive culture. *Proceedings of the Ninth International Symposium on Human Aspect of Information Security & assurance aspect* (pp. 1-276). College of Science. Engineering and Technoloogy . School of Computing . University of South Africa.

Da Veiga, A. (2016). Comparing the information security of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information and Computer Security, 24*, 139-151.

Da Veiga, A. (2019). Achieving a Security culture. *In Cybersecurity education for awareness and compliance*, pp 72-100. IGI Global.

Da Veiga, A., & Eloff, J. (2010, March). A framework and assessment instrument for information security culture. *Computer and Security, 29*(2), 196-207.

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

Da Veiga, A., & Martin, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers and Security, 49*, 162-176.

Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture- A validated assessment instrument. *Computer Law and Security Review, 31*, 243-256.

Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers and Security, 70*, 72-94.

Da Veiga, A., Astakhova, L., Botha, A., & Herselman, M. (2020, May). Defining organisational information security - Perspectives from academia and industry. *Computers and Security, 92*, 1-22.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the security literature: making sense of the disparate findings. *European Journal of Information Systems, 20*(6), 643-658.

D'Arcy, J., & Hovav, A. (2009). Does on size fitall? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics, 89*(1), 59-71.

De Benetti, T. (2014). *Theory's role in a Research.* Carrolton, United States: Researchgate.

De Lange, J., Von Solms, R., & Geber, M. (2015). Better information security management in municipalities. *IST - Africa Conference.* Lilongwe: IEEE.

De Vos, A., Strydom, H., Fouche, C., & Delport, C. (2005). *Research at Grass Roots for the Social Sciences and Human Service Professions* (3 ed.). Pretoria: Van Schaik.

Dhakal, R. (2018). *Measuring the Effectiveness of an Information Security Training and Awareness Program.* Charles Sturt University, Sydney.

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers and Security, 56*, 63-69.

Djerouni, M. (2019). Implications of employees in security policies definition. *International Journal of Information Security and Cybercrime (IJISC)*, 8(1), 23-29.

Doherty, N., & Tajuddin, S. (2018). Neil F. Doherty, Sharul T. Tajuddin. *Towards a user-centric theory of value-driven information security compliance, 31*(2), 348-367.

Eastern Cape Provincial Treasury. (2014). *Information Technology Audits.* East London: Transversal Internal Audits.

Eastern Cape Provincial Treasury. (2015). *Information Technology Audits.* East London: Transversal Internal Audits.

Eastern Cape Provincial Treasury. (2016). *Information Techonology Audits.* East London: Transversal Internal Audits.

Eastern Cape Provincial Treasury. (2017). *Information Technology Audits.* East London: Transversal Internal Audits.

ECD. (2015). *ECD Global Infotech: Ensuring Information Security with Cyber Security Risk and Assurance services*. Retrieved 2016, from The Information Security Practitioners: https://cyber-security.cioreviewindia.com/vendor/2015/ECD_Global_Infotech

Eloff, M., & Von Solms, S. (2000). Information security management: an approach to combine process certifation and product evaluation. *Computers & Security, 19*, 698-709.

ENISA. (2017). *Mapping of OES Security Requirements to Specific Sectors.* European Network and Information Security .

Ernst & Young. (2019). Get Ahead of Cybercrime - EY's Global Information Security Survey 2014. *Insight on Risk, governance and Compliance*.

European Network and Information Security Agency. (2017). *Information security awareness: Local government and internet service providers.* ENISA.

European Union Agency For Network and Information Security. (2017). *Cyber Security Culture in organisations.* ENISA.

Farquhar, J. (2018). *Case Study Research for Business.* London: SAGE Publications.

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

Flick, U. (2018). An introduction to qualitative research. Sage Publishers.

Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59*, 26-44.

Furnell, S., & Clarke, N. (2015). Human Aspects of Information Security and Assurance. *Proceedings of the Ninth International Symposium on Human Aspects of Information security and Assurance* (pp. 1-276). Plymouth: Centre for security, Communication and Nertwork Research.

Fusch, P., Fusch, G. E., & Ness, L. R. (2018). Denzin's paradigm shift: Revisiting triangulation in qualitative research. *Journal of social change, 10*(1), 2.

Gangire, Y., Da Veiga, A., & Herselman, M. (2019). A conceptual model of information security compliant behaviour based on the self-determination theory. *2019 Conference on Information Communications Technology and Society (ICTAS)* (pp. 1-6). Pretoria: IEEE.

Gebrasilase, T., & Lessa, L. (2017). Information Security Culture in Public Hospitals: The Cse of Hawas Referral Hospital. *The African Journal of Information Systems, 3*(3), 72-86.

Ghazvini, A., & Shukur, Z. (2017). Information Security Content Development for Awareness Training programs in healthcare. *International Journal of Security and Its Applications, 11*(7), 87-96.

Giandomenico, N., & De Groot, J. (2018). Insider vs.Outsider Data Security Threats: What's the Greater Risk? *Data Protection*.

Gilbert, C. (2017). *Developing an integrated security training, awareness, and education program.*

Haeussinger, F., & Kranz, J. (2018). Information security awareness: Its antecedents and mediating effects on security compliant behaviour. *In: Proceedings of the International Conference on Information Systems ICIS*, (pp. 1-12). Milan, Italy.

Hamid, H., & Dali, N. (2020). Empirical Study on the influence of security control management and social factors in deterring information security behaviour. *Journal Physics: Conference Series, 1551*(1), 12010.

Harding, J. (2018). *Qualitative data analysis: From start to finish* (2nd ed.). London: Sage.

Harrison, R. (1972, February). *harrisons-model-of culture.* Retrieved 2014, from https://research-methodology.net/.

Hassan, N., Mingers, J., & Stahl, B. (2018). Philosophy and information systems: where are we and where should we go? *European Journal of Information Systems*.

Hassandoust, F., & Techatassanasoontorn, A. A. (2020). Understanding users'information security awareness and intentions: A full nomology of protection motivation theory. *In Cyber Influence and Cognitive Threats*, 129-143.

Herath, T., & Rao, T. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*, 154–165.

Hina, S., & Dominic, P. (2018). Information security policies' compliance: a perspective for higher education institutions, Journal of Computer Information Systems. *Journal of Computer Information Systems*, 1-11.

Hofstede, G. (2017). Organisational culture. Retrieved from https://geert-hofstede.com/organisational-culture.html

Hogan, S., & Coote, L. (2013). Organisational culture, innovation, and performance: A test of Schein's model,. *Journal of Business Research*, 1-13.

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

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2021). Security Awareness: The First Step in Information Security Compliance Behaviour. *Journal of Computer Information Systems, 61*(4), 345-356.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. *Comput. Secur., 31*(1), 83-95.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management, 51*(1), 69-79.

Ismail, N., Kinchin, G., & Edwards, J. A. (2018). Pilot study, does it really matter? Learning lessons from conducting a pilot study for a qualitative PhD thesis. *International Journal of Social Science Research, 6*(1), 1-17.

ISO 31000. (2018). Risk Management Guidelines. *International Orgranisation for Standardisation*. Available at: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

ISO/IEC 27013. (2021). Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1. *International Organisation for Standardisation*. Available at: https://www.iso.org/obp/ui#iso:std:iso-iec:27013:ed-3:v1:en

Jaeger, L. (2018). Information Security awareness: literature review and integrative framework. *Proceedings of the 51st Hawaii International Conference on System Sciences* (pp. 4703-4712). Hawaii: HICSS.

Johnson, M., & Goetz, E. (2007). Managing Organisational Security - Embedding Information Security into the Organization. *Security and Privacy*, 16-24.

Joshi, C., & Singh, U. (2017). Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications, 35*, 128-137.

Jouinia, M., Rabaia, L., & Aissa, A. (2018). Classification of security threats in information systems. *5th International Conference on Ambient Systems, Network and Technologies (ANT-2014). 32*, pp. 489-496. Tunis: Elsevier.

Karlsson, M., Denk, T., & Åström, J. (2018). Perceptions of organizational culture and value conflicts in information security management. *Information and Computer Security, 26*(2), 213-229.

Karokola, G. (2012). *A framwework for securing e-government services - The case of Tanzania.* Stockholm University, Computer and Systems Sciences. Sweden: US-AB.

Karyda, M. (2017). Fostering information security culturein organisations: A research agenda. *The 11th Mediterranean Conference on Information systems (MCIS)* (pp. 1-11). Genoa, Italy: Association for Information Systems.

Kassem, R., Angappa, M., & Helo, G. (2018). Assessing the impact of organizational culture on achieving business excellence with a moderating role of ICT: An SEM approach. *Benchmarking: An International Journal*, 1-31. doi:https://doi.org/10.1108/BIJ-03-2018-0068

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic Literature Review. *Computers & Security*, 102267.

Kivunja, C., & Kuyini, A. (2017). Understanding and applying research paradigms in educational contexts. *International Journal of Higher Education, 6*(5), 26-41.

Klein, H., & Myers, M. (2001). A Classification Scheme for Interpretive Research in Information Systems. In E. Trauth, *Qualitative Research in IS: Issues and Trends* (pp. 218-239).

Knapp, K., Marshall, T., Rainer, R., & Ford, F. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security, 14*(1), 24-36.

Kolkowaska, E., Karlsson, F., & Hedstrom, K. (2017). Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. *The Journal of Strategic Information Systems, 26*(1), 39-57.

Koohang, A., Anderson, J., Nord, J., & Paliszkiewicz, J. (2019). Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems, 120*(1), 231-247. Retrieved 2020

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice, 24*(1), 120-124.

Kostadinov, D. (2014). Key Elements of an information security policy . *General Security, Incident Response*. Retrieved from http://resources.infosecinstitute.com/key-elements-information-security-policy/

Kraus, P. (2018, September). *Data Protection.* Retrieved from Digital Guardian.

Kritzinger, E., Bada, M., & Nurse, J. (2017). A study into the cybersecurty awareness initiativesfor school learners in South Africa and the UK. *IFIP World Conference on Information Security Education*, 110-120.

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The utility of information securty training and education on cybersecurty incidents: an empirical evidence. *Information systems Frontiers, 23*(2), 361-373.

Labuschagne, L. (2017). Cyber security awareness: the first and most important line of protection. *Training and e-Learning*. Retrieved from https://www.itweb.co.za/: https://www.itweb.co.za

Lebek, B., Uffen, J., Breitner, M., & Neumann, M. a. (2013). Employees' information security awareness and behaviour: A litreature review. *International Connference on System Scienes. 46*, pp. 2978-2987. Hawaii: HCISS.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. (2019). Information security awareness and behaviour: a theory based literature review. *Management Research Review, 37*(12), 1049-1092.

Lemon, L. L., & Hayes, J. (2020). Enhancing trustworthiness of qualitative findings: Using Leximancer for qualitative data analysis triangulation. *The Qualitative Report, 25*(3), 604-614.

Li, Y., Stafford, T., Fuller, B., & Ellis, S. (2017). Beyond Compliance: Empowering Employees' Extra-Role Security Behaviours in Dynamic Environments. *AMCIS 2071 Proceedings*, (pp. 1-5).

Linneberg, M., & Korsgaard, S. (2019). Coding qualitative data: A synthesis guiding the novice. *Qualitative research journal., 19*(3), 259-270.

Lishner, D. (2015). A concise set of core recommendations to improve the dependability of psychological research. *Review of General Psychology, 19*(1), 52-68.

Lohrmann, D. (2018, March 9). Ten Recommendations for Security Awareness Programs. *Lohrmann on Cybersecurity and Infrastructure*. Retrieved from https://www.govtech.com/blogs/lohrmann-on-cybersecurity/Ten-Recommendations-for-Security-Awareness-Programs.html.

Mahfuth, A., Yussof, S., Baker, A., & Ali, N. (2017). A systematic literature review: Information security culture. *International Conference on Research and Innovation in Information Systems (ICRIIs)*, 1-6.

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security awareness on privacy -protective behaviours. *Computers in human behaviours, 83*, 32-44.

Martella, R., Nelson, R., & Marchand-Martella, N. (1998). *Research Methods -Learning to Become a Critical Research Consumer.* Boston: Allyn and Bacon.

Martins, A., & Eloff, J. (2002). Information security culture. *Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives.* Auckland Park: International Federation for Information Processing.

Ma'ruf, K., & Rochman, M. (2019). Guidelines for developing information security training and awareness programs in government agency: The perspective of ADDIE instructional design models (A Case study in Indonesian government agency. *PEOPLE: International Journal of Social Sciences, 5*(2), 863-877.

Masrek, M., Harun, Q., & Sahid, N. (2018). Assessing the information security culture in a Government Context: The Case of a Developing Country. *International Journal of Civil Engineering and Technology, 9*(8), 96-112.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behaviour, 69*, 151-156.

McCue, D., & Tartaglia, A. (2010). Self-report response bias: Learning how to live with it diagnosis in chaplincy research. *Chaplaincy today- E.Journal of association of professional chaplains, 26*(1), 1-7.

McIlwraith, A. (2016). *Information security and employee behaviour: How to Reduce Risk Through Employee Education, Training and Awareness* (1st ed.). London: Routledge . doi:https://doi.org/10.4324/9781315588537

Menard, P., Bott, G., & Crossler, R. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *Journal of Management Information Systems, 34*(4), 1203-1230.

Metalidou, E., Marinagi,C., Trivellas, P., Eberhagen,N., Skourlas, C., & Giannakopoulos,G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia - Social and Behavioural Sciences, 147*, 424-428.

Meyer, B. (2015). *Researching Translation and Interpreting.* London: Imprint Routledge.

Michalsons, M. (2017, February 28). Minimum Information Security Standards (MISS). *Information Security Law*.

Miles, M., Huberman, M., & Saldana, J. (2018). *Qualitative Data Analysis; A Methods Sourcebook.* British Columbia: SAGE Publications.

Moody, G., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1), 285-335.

Moon, M. (2019). Triangulation: A method to increase validity, reliability, and legitimation in clinical research. *ournal of Emergency Nursing, 45*(1), 103-105.

Moore, E., & Llompart, J. (2017). Collecting, transcribing, analyzing and presenting plurilingual interactional data. *Qualitative approaches to research on plurilingual education*, 403-417.

Mousavi, M., & Kumar, S. (2019). Analysis of key factors for organisation information security. *International Conference on Machine Learning, Big Data, Cloud and Parallel Computing*, 514-518.

Myers. (1997). Interpretive Research in Information Systems. In J. Mingers, & F. Stowell, *Information Systems: An Emerging Discipline?* (pp. 239-266). London: McGraw-Hill.

Nasir, A., Arshah, R., & Hamid, M. (2019). A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions. *Information Security Journal: A Global Perspective, 28*(3), 55-80.

Nasir, A., Arshar, R. A., & Ab Hamid, M. R. (2017). Information Security Policy Compliance Behaviour Based on Comprehensive Dimensions of Information Security Culture: A Conceptual Framework. *Association for Computing Machinery*, 56-60.

Nasir, A., Arshar, R., & Hamid, M. (2017). Information Security Policy Compliance behaviour based on comprehensive dimensions of information security culture: A conceptual framework. *Association for Computing Machinery, 1*, 56-60.

Nasir, A., Arshar, R., Ab Hamid, M., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A revies. *Journal of Information security and applications, 44*, 12-22.

National Center for Education Statistics. (2019, May 19). Safeguarding your technology. *Security Policy: Development and Implementation*, pp. 1-8.

Ndiege, J., & Okello, G. (2018). Information security awareness amongst students joining higher education institutions in developing countries: Evidencefrom Kenya. *The African Journal of Information Systems, 10*(3), 204-221.

Nel, F. (2017). *Determining a standard for information security culture.* Computer Science. Potchefstroom: North West University.

Nel, F., & Drevin, L. (2019). Key elements of an information security culture in organisations. *Information and computer security, 27*(2), 146-164.

Nestel, D., Hui, J., Kunkler, K., Scerbo, M., & Calhoun, A. (2019). *Healthcare Simulation Reseaarch - A Practical Guide.* Swirtzerland: Springer.

Newton, N., Anslow, C., & Drechsler, A. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *National Institute of Standards and Technology (NIST) special publication 800*, 181.

Newton, N., Anslow, C., & Drechsler, A. (2019). Information Security in Agile Software Development Projects: a Critical Success Factor Perspective. *27th European Conference on Information Systems (ECIS).* Sweden: Stockholm & Uppsala.

Nieles, M., Depmpsey, K., & Pillitteri, Y. (2017). An Introduction to Information Security. *NIST Special Publication 800-12 Revision*, 1-97.

NIST Special Publication 800-37. (2018). Guide for Applying the Risk Management Framework to Federal Information Systems. NIST website. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Oates, B. (2006). *Researching Information Systems and Computing* (1 ed.). London: Sage Publications.

O'Brien, J., Islam, S., Weng, F., Xiong, W., & Ma, A. (2018). InformationSecurity Culture: Literature Review. *Working Paper*.

Okere, I., Van Niekerk, J., & Carroll, M. (2017). Assessing Information Security Culture: A Critical Analysis of Current Approaches. *Information Security for South Africa*, 1-8.

Pahnila, S., Siponen, M., & Mahood, A. (2007). Employees' behaviour towards IS security policy compliance. *Proeceeds of the 40th Hawaii International Conference on System sciences* (pp. 1-10). Big Island.

Palega, M., & Knapinsski, M. (2019). Assessment of employees level of awareness in the aspect of information security. *System Safety: Human-Technical Facility-Environment, 1*(1), 132-140.

Paliszkiewicz, J. (2019). Information Security Policy Compliance: Ladership and Trust. *Journal of Computer Information Systems*, 1-8.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The hyman aspect of information security Questionnaire (HAIS-Q) ; Two further validation studies. *Computers and security*, 40-51.

Parsons, K., McCormac, A., & Butavicius, M. (2016). The development of the human aspect of information security questionnaire (HAIS-Q). *24th Australasian Conference on Inforomation Systems Human Aspects of InfoSec*, 1-11.

Parsons, K., Young, E., Butavicius, M., McCormac, A., Pattinson, M., & Jerram, C. (2015). The influence of organisational information security culture on information security decision making. *Journal of cognitive engineering and decision making, 9*(2), 117-129.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2016). A study of information security awareness in Australian government organisations. *Information Management & Computer Security, 22*(4), 334-345.

Pattabiraman, A., Srinivasan, S., Swaminathan, K., & Gupta, M. (2018). Fortifying corporate human wall: A litereature review of security awsreness and training. *Information Technology Risk Management and Compliance in Modern Organisations*, 142-175.

Patton, M. (2018). *Qualitative Research and Evaluation Methods: Integrating Theory and Practice.* London: SAGE Publications.

Pazur, M. (2020). Development and validation of a research instrument for measuring the presence of democratic school leadership characteristics. *Educational Management Administration & Leadership*, 1-17.

PCI security Standards Council. (2014, October). Best Practices in Organisational Security Awareness. *Security Awareness Porgram Special Interest Group*.

Pfleeger, C., Pfleeger, S., & Margulies, J. (2016). *Security in computing* (5th ed.). Upper Saddle River, New Jersey: Prentice Hall.

Phillips, W. (2017). Research tools: interviews and questionnaires. *Research Methodology in Education*, 1-15.

Queirós, A., Faria, D., & Almeida, F. (2017). Strengths and Limitations of Qualitative and Quantitative Research Methods. *European Journal of Education Studies, 9*(3), 369-406.

Raikkonen, I. (2017). Motivations behind employee information security behaviour. University of Jyväskylä.

Rechberg, I. (2018). Knowledge Management Paradigms, Philosophical Assumptions: An Outlook on Future Research. *American Journal of Management, 8*(3), 61-74.

Robson, C. (1993). *Real World Research: A Resource for Social Scientists and Practitioner-Researchers.* Paris: Blackwell Publishing.

Ruighaver, A., Maynard, S., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security, 26*, 56-62.

Safa, N., Sookhak, R., Von Solms, R., Furnell, S. N., & Herawan, T. (2015). Information security conscious care behaviour formation in organisations. *Computers & Security, 53*, 65-78.

Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organisations. *Computers & Security*, 70-82.

Saint-Germain, R. (2017). Information Security Management Best Practice Based on ISO/IEC 17799. *The Information Management Journal*, 60-66.

SANS Security Awareness Report. (2019). *SANS Security: Value of Managing Human Risk for Leadership.* SANS.

Sarala, R., Zayaraz, G., & Vijayalakshmi, V. (2016). Optimal Selection of Security Countermeasures for Effective Information Security. *Proceedings of the International Conference on Soft Computing Systems. Advances in Intelligent Systems and Computing. New Delhi. 398*, pp. 345-353. New Delhi: Springer.

Saunders, M., Lewis, P., & Thornhill, A. (2009). Understanding research philosophies and approaches. *Research Methods for Business Students., 4*, 106-135.

Schein, E. (1992). *Organisational culture and leadership.* California: Jossey-Bass.

Schein, E. (2004). *Organisational culture and Leadership* (3rd ed.). San Francisco: Jossey-Bass.

Schlienger, T., & Teufel, S. (2003). Information security culture - From Analysis to change. *3rd Annual Information Security South Africa Conference*, (pp. 183-195). Sandton Convention: Johannesburg.

Schultz, E. (2005). The human factor in security. *Computers & Security, 24*(6), 425-426.

Sestak, J., & Sestak, J. (2010). Chapter 6. Research design. *Reseach Desin, 6*, 189.

Shamala, P., Ahmad, R., Zolait, A., & Sedek, M. (2017). Integrating information quality dimensions into information security risk management. *Journal of Information Security and Applications, 36*, 1-10.

Shameli-Sendi, A., Aghababaei-Beazegar, R., & Cheriet, M. (2016, March). Taxonomy of information security risk assessment (ISRA). *Computers & Security, 57*, 14-30.

Shenton, A. (2004). Strategies for ensuring trustiworthiness in Qualitative research projects. *Education for Information*, 63-75.

Sherif, E., Furnell, S., & Clarke, N. (2016). An identification of Variables Influencing the Establishment of Information Security culture. *International Conference on Human Aspects of Information Security , Privacy Trust*, (pp. 436-448). Port Elizabeth.

Shouran, Z. (2019). Information System Security: Human Aspects. *International journal of scientific & technology research, 8*(03), 111-115.

Sibona, C., Walczak, S., & White Baker, E. (2020). A guide for purposive sampling on twitter. *Communications of the association of information systems, 46*(1), 22.

Silverman, D. (2011). *Interpreting Qualitative Data - A guide to the Principles of Qualitative Research.* London: Sage.

Simon, & Goes. (2012). Sample Size Matters: What type of cook (reseacher) are you? *Dissertation and Schorlaly Research: Recipes for Success*, pp. 1-10.

Singh, A., Gupta, M., & Ojha, A. (2016). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management, 27* (5), 644-667.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Siponen, M., & Vance, A. (2016). Neew Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly, 34*(3), 487-502.

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

Sohrabi, N., Sookhak, M., Von Solms, R., Furnell,S., Ghani, N.A, & Herawan,T. (2015). Information security conscious care behaviour formation in organizations. *Computers and security, 53*, 65-78.

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

Spacey, J. (2016, June 27). *The Big list of information security vulnerabilities*. Retrieved from Simplicable: https://arch.simplicable.com/arch/new/the-big-list-of-information-security-vulnerabilities

Stake, R. (1995). *The art of case study research.* Thousand Oaks: London: Sage Publications.

Stake, R. (2005). Qualitative Case Studies. In N. Denzin, & Y. Lincoln, *The Sage handbook of qualitative research* (pp. 443-466). Sage Publications Ltd.

Stefaniuk, T. (2020). Training in shaping employee information security awareness. *Entrep. Sustain, 7*.

Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security: a case study. *Information Technology Management, 17*, 179-186.

Thomas, P. (2010). towards developing a web-basedblended learningenvironment at the University of Botswana. University of South Africa. Pretoria.

Thomson, K., & Van Niekerk, J. (2016). Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management& Computer, 20*(1), 39-46.

Thomson, K., Von Solms, R., & Louw, L. (2006). Cultivating an organisational information security culture. *Computer Fraud & Security*, 7-11.

Tolah, A., Furnell, S., & Papadaki, M. (2017). A comprehensive Framework for Cultivating and Assesing Information Security Culture. *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurane*, 52-64.

Tsohou, A., Karyda, A., Kokolakis, S., & Kiountouzis, E. (2018). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems, 24*(1), 38-58.

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the intrnalisation of information security policies: Recommendations for information security awareness programs. *Computers and Security, 52*, 123-141.

Van Niekerk, J., & Von Solms, R. (2005). Aholistic framework for the fostering of an information security sub-culture in organisations. *4th Annual ISSA Conference*.

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

Vance, A. (2010). *Why do employees violate IS Security Policies? Insights from multiple theoretical perspectives.* Finland: University of Oulu.

Vance, A., Siponen, M., & Pahnilla, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management, 49*(3-4), 190-198.

Verizon. (2021). *2021 Data Breach Investigations Report.* Retrieved from https://www.researchgate.net/publication/351637233_2021_Verizon_Data_Breach_Investigations_Report/link/60a2a6cd92851cd4566b444e/download

Vijayan, J. (2018). Security Imperative. *Computer World*, 1-2.

Von Solms, R. V., & Von Solms, B. (2004). From policies to culture. *Computers & Security, 23*, 275-279.

Wahyudiwan, D., Sucahyo, Y., & Gandhi, A. (2017). Information Security Awareness Level Measurement: for Employee:. *3rd International Conference on Science in Information Technology (ICSITech)* (pp. 654-658). Indonesia: IEEE.

Whitman, M., & Mattord, H. (2018). *Principles of Information Security.* Boston: Cengage Learning.

Whitman, M., & Mattord, H. (2016). Threats to information Protection -Industry and Academic Perspectives: An annotated bibliography. *Journal of Cybersecurity Education, Research and Practice, 2*, 1-4.

Whitman, M., & Mattord, H. (2021). *Principles of incident response and disaster recovery* (Fifth ed.). Boston: Cengage Learning.

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security, 88*, 1-8.

Wilson, M., & Hash, J. (2003). Building an Information Technology Security Awareness and Training Program -NIST Special Publication 800-50. *National Institute of Standardz and Technology*. Retrieved from http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=151287

Wu, Y., Stanton, B., Galbraith, J., & Cole, M. (2018). Protection Motivation theory and adolescent drug trafficking: Relationship between health motivation and longitudinal risk involvement. *Journal of Pediatric Psychology, 30*(2), 127-137.

Wu, Y., Stanton, B.F., Li, X., Galbraith, J., & Cole, M.L. (2005). Protection motivation theory and adolescent drug trafficking: Relationship between health motivation and longitudinal risk involvement. *Journal of Pediatric Psychology, 30*(2), 127-137.

Yin, R. (2018). *Case Study Research and Applications: Design and Methods* (6th ed.). Los Angeles: SAGE Publications.

Zakaria, O., & Gani, A. (2003). A Conceptual checklist of information Security Culture. *Proceedings of the 2nd European Conference on Information Warfare and security*, (pp. 365-371). United Kingdom.

Appendix A: Certificate of Approval

University of Fort Hare
Together in Excellence

ETHICS CLEARANCE REC-270710-028-RA Level 01

Project Number:	BOU021SPOT01
PROJECT TITLE:	**A FRAMEWORK FOR PREPARING AN INFORMATION SECURITY AWARENESS PROGRAMME: A CASE OF THE EASTERN CAPE PROVINCIAL GOVERNMENT.**
Qualification:	Masters in Information Systems (Full Dissertation)
Student name:	Zandile Potelwa
Registration number:	201600492
Supervisor:	Mr. D Boucher
Department:	Information Systems
Co-supervisor:	N/A

On behalf of the University of Fort Hare's Research Ethics Committee (UREC) I hereby grant ethics approval for **BOU021SPOT01**. This approval is valid for 12 months from the date of approval. Renewal of approval must be applied for BEFOREtermination of this approval period. Renewal is subject to receipt of a satisfactory progress report. The approval covers the undertakings contained in the above-mentioned project and research instrument(s). The research may commence as fromthe 03/11/20, using the reference number indicated above.

Note that should any other instruments be required or amendments become necessary, these require separate authorisation.

Please note that UREC must be informed immediately of

- Any material changes in the conditions or undertakings mentioned in the document;
- Any material breaches of ethical undertakings or events that impact upon the ethical conduct of the research.

The student must report to the UREC in the prescribed format, where applicable, annually, and at the end of the project, in respect of ethical compliance.

UREC retains the right to

- Withdraw or amend this approval if
    - Any unethical principal or practices are revealed or suspected;
    - Relevant information has been withheld or misrepresented;
    - Regulatory changes of whatsoever nature so require;
    - The conditions contained in the Certificate have not been adhered to.

- Request access to any information or data at any time during the course or after completion of the project.

Your compliance with Department of Health 2015 guidelines and any other applicable regulatory instruments and with UREC ethics requirements as contained in UREC policies and standard operating procedures is implied.

UREC wishes you well in your research.

Yours sincerely

PROFESSOR RENUKA VITHAL
Chairperson: University Research Ethics Committee

22 February 2021

Appendix B: Interview Guide

Research Instrument for the Masters Dissertation titled:

A framework to prepare an information security awareness and training programme: A case of the Eastern Cape provincial government

---

Interview preamble

The following questions focus on clarifying potential determinants of an Information Security Awareness program for Eastern Cape Provincial departments.

Interview Questions

1. Organisational Information security culture

What do you think of when you hear the term *information security*?
Prompt 1: How might information security be applicable in your personal life?
Prompt 2: How might information security be relevant in your work life?

1. 1 In your opinion, how important is *information security* in the management practices of your department?
Prompt 1: Are you able to provide some examples where management has raised issues around *information security*?
Prompt 2: Are you encouraged in the workplace to follow "good" information security practices provided by management?

1.4. What activities (if any) does your department do to promote *information security awareness* amongst its employees?
Prompt 1: Is an effort made to make employees aware of *information security* related policies, which might impact their daily job?
Prompt 2: Are employees made aware of any compliance requirements associated with information security policies?

1.5. When having strategic planning sessions does your department include the protection of information as part of the discussions?
Prompt 1: What information security strategy (if any) is put in place to protect information assets?
Prompt 2: In your opinion, how can your department include the protection of information assets during the planning sessions?

1.6. What continuity processes are you aware of if a disaster (human or otherwise) strikes the information assets of the department?
Prompt 1: Are you aware of any documented processes?
Prompt 2: Have any continuity plans been communicated to employees?

3. Information Security risks and threats

What is your specific role in the department, how do you perceive information security risks within your department?

2.6. Do you know where to get a copy of information security policies (if it exists) for your department?

Prompt 1: Have you read any rules or policies regarding information security?
Prompt 1.1: If no – prompt – is there any specific reason why you have not done so? Why not?
Prompt 1.2: If yes, were these understandable?

2.7. Have you been informed of information security requirements in the last twelve months?
Prompt 1: For example regulations regarding downloading of email attachments from unknown sources.
Prompt 1.1: If yes, how do you comply with these requirements?

2.8. What do you understand as an information security incident in the workplace?
Prompt 1: Are you able to share an example that may have happened in the last 12 months that you are aware of?

2.9. *Information security breaches occur when an intruder gains unauthorised access to your department's protected systems and data.* What measures are you aware of that your department is taking to ensure that there are no security breaches?

2.10. What information security threats are employees exposed to in relation to information assets?
Prompt 1: How does the department reduce information security threats?
Prompt 1.1: For example, weak passwords, or unauthorised installation of an application on the computer, or uninstalled updates?

3. Employees' perceptions about information security

3.9. How do you feel that employees can comply with the requirements of your department's information security policy?

3.10. What is your view on the measures put in place by your department to reduce the chance of information security threats?
Prompt 1: For example, some companies require staff to change a password on monthly basis?
Prompt 2: For example, are you able to download work related content and take it away from the office to work on it?
Prompt 2.1: How do you protect the data when it is in your possession?
Prompt 2.1.1: For example, from theft, unauthorised access?

3.11. Suppose that in your department security awareness of information security policy has been conducted and an employee does not abide by information security rules as outlined in the security policy, and there is a breach:
Prompt 1: What actions do you think the department should take against such an employee?

3.12. Do you think your department could be vulnerable to information security threats?
Prompt 1: What leads you to this conclusion?

3.13. How do you think an employee can become knowledgeable about information security policies and guidelines?
Prompt 1: Are there any aspects that you think might complicate employees getting the knowledge about information security policies in the workplace?

3.14. How confident are you that you can comply with information security policies?
Prompt 1: Why do feel that way?

3.15. What sanctions are in place by if information security policies are violated?
Prompt 1: If those sanctions are severe, are employees likely to change their information security behaviour? What makes you think so?

3.16. What can promote better security behaviour among employees in your department?

4. Security Awareness

What is your specific role in the department? How do you perceive the department's ISA programmemes

4.1. Does your Department conduct information security awareness training sessions?

Prompt 1 - **YES**: What types of topics are covered in the training sessions?
Prompt 1.1: Are you aware of your Department budgeting money and time for information security awareness related training?
Prompt 1.2: Is ongoing information security awareness training part of the employee development in your Department?
Prompt 1.2.1: How is it / should it be done?
Prompt 1.3: Is the training offered in-house by the Department or offered by an external vendor (outsourced)?
Prompt 1.3.1: If the training is offered by an external vendor, how is it tailored to your day to day job?
Prompt 1.3.2: What do you feel is the best way for training to be delivered to you in the workplace? For example, face-to-face training, online videos, computer-based training?
Prompt 1.4: How do you make sure that specific information security training is attended by relevant employees?

Prompt 2 - **NO**: What types of topics do you think should be included in such training, if it were offered?
Prompt 2.1: What would you want to know more about from an information security point of view?

Thank you for taking the time to help me understand your working environment and the impact of information security awareness.

University of Fort Hare
Together in Excellence

INDIVIDUAL INFORMATION SHEET AND INFORMED CONSENT FORM[2]

(AGES 18 YEARS AND ABOVE)

Title of Study:

A framework for preparing an information security awareness programme: A case of the Eastern Cape provincial government

Ethical Clearance Number: BOU021SPOT01

Dear participant,

My name is [ZANDILE POTELWA] and I am studying at the University of Fort Hare towards a MASTER OF COMMERCE IN INFORMATION SYSTEMS. The qualificaiton requires me to complete a research study on an approved topic. The **Purpose of Research Study** is to produce a framework to be used to prepare an information security awareness programme for Eastern Cape Provincial departments.

I would like you to participate in a brief, approximately 1 hour, interview where I will ask you some questions about your understanding and experiences with information security within your work environment. Your input will give me a better idea of what information security issues arise in your workplace.

You may consider some questions as being of a personal and/or sensitive nature. If you feel that any question may be too personal for you to answer or might make you uncomfortable, then simply tell me you are unwilling to answer that question. I will be asking some questions that you may not necessarily have thought about before this interview. I know that you cannot be absolutely certain about the answers to these questions, but I ask that you try to think about these questions. When it comes to answering questions there are no right and wrong answers.

Please understand that **your participation is voluntary** and you are not being forced to take part in this study. The choice of whether to participate or not, is yours. However, I would really appreciate it if you do share your thoughts with me. If you choose not to take part, you will not be affected in any way whatsoever. If you agree to participate, you may stop me at any time and tell

[2] Approved by UREC (13 November 2019)

me that you don't want to go on with the interview. If you do this there will also be no penalties and you will NOT be prejudiced in ANY way.

The interview and any information shared will confidential. This means that no identifying information such as your name or Department details will be linked in any way to the answers you give. I will study and report on the answers given by all the participants that I interview and not on an individual basis. The research data will be anonymised – with all personal respondent information being removed and your interview responses will be securely archived (using password protection) with the Department of Information Systems at the University.

At the present time, I do not see any risks in your participation. The risks associated with participation in this study are no greater than those encountered in daily life. There are also no immediate benefits to you from participating in this study. However, this study will be helpful in finding out *the activities performed by employees and employers to address information security, risks and controls ; the factors required for the preparation of an information security awareness program for public sector employees; and the requirements to be considered when building information security culture in provincial government departments*.

This research has been approved by the Inter-Faculties Research Ethics Committee (IFREC) as per delegated authority of the University Research Ethics Committee (UREC). If you have any complaints about ethical aspects of the research or feel that you have been harmed in any way by participating in this study, please contact the IFREC Administrator on researchethics@ufh.ac.za.

Reporting and Complaints

If you have questions at any time about this study, or if you have concerns/questions you may contact the researcher/project leader whose contact information is provided on the first page. If you have questions regarding your rights as a research participant, or if problems arise which you do not feel you can discuss with the researcher/project leader, please contact the IFREC Chairperson, Prof. Munacinga Simatele on researchethics@ufh.ac.za or the UREC Chairperson, Prof. Renuka Vithal on researchethics@ufh.ac.za.

If you have concerns or questions about this study please feel free to contact the project coordinators: **Researcher/Project Leader:**

Name: Zandile Potelwa

Department: Information Systems

INFORMED CONSENT FORM

I _____ have been informed about the study by ZANDILE POTELWA.

I understand the purpose, procedures, and the potential risks and benefits of the study.

I have been given an opportunity to ask questions about the study and have had answers to my satisfaction.

I declare that my participation in this study is entirely voluntary and that I may withdraw at any time.

I understand that I will be given a copy of this informed consent form.

I understand that if I have any questions or complaints about my rights as a study participant, or if I may have concerns about any aspect of the study or the researcher then I may contact the Chairperson of the Inter-Faculty Research Ethics Committee, Prof. Munacinga Simatele or Chairperson of University Research Ethics Committee, Prof Renuka Vithal (details available from the Researcher or by contacting the University of Fort Hare or Website www.ufh.ac.za)

Participant signature:

Consenting for Audio Recording: Do you agree to the recording of your interview session in order to allow the researcher to make accurate transcripts of your responses? YES / NO

Participant signature:

Data storage: I understand that the information that I provide will be stored electronically and will be used for research purposes now or at a later stage (to be altered according to the study)

Participant signature:

Date: