

The Effects of Cultural Contradictions on **Information Security Compliance** **Behaviour**

A research outline presented to the

Department of Information Systems

University of Cape Town



by

Grant Solomon

(Student Number: SLMGRA002)

in partial fulfilment of the requirements for the course of
Masters of Commerce Degree in Information Systems (INF5000W)

2023

Supervisor: Professor Irwin Brown

Co-Supervisor: Doctor Sharon Geeling

The copyright of this thesis vests in the author. No quotation from it or information derived from it is to be published without full acknowledgement of the source. The thesis is to be used for private study or non-commercial research purposes only.

Published by the University of Cape Town (UCT) in terms of the non-exclusive license granted to UCT by the author.

Declaration

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.
2. I have used the APA convention for citation and referencing. Each contribution to, and quotation in, this paper entitled **The Effects of Cultural Contradictions on Information Security Compliance Behaviour** from the work(s) of other people has been attributed and has been cited and referenced.
3. This paper is my own work, part of which appeared in an earlier Research Proposal submitted to the University of Cape Town.
4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work
5. I acknowledge that copying someone else's assignment, essay or paper, or part of it, is wrong, and declare that this is my own work.

Signature(s)

Signed by candidate

Date 29/08/2023

Full name(s) of student(s)

Grant Solomon



Acknowledgements

First and foremost, I would like to express my gratitude to my Lord and Saviour, Jesus Christ, for granting me the strength and ability to complete this dissertation.

To my wife, Naomi Solomon, thank you for your sacrifice and the part you played in completing this dissertation.

To my supervisors, Professor Irwin Brown and Doctor Sharon Geeling, your expert guidance and continual support have been invaluable throughout this journey.

To my parents who never stopped believing in me, thank you for your continuous encouragement.

Finally, to all the research participants who were interviewed, thank you for your time and input.

Abstract

Purpose: Organisational culture and an information security subculture can have a significant influence on employee compliance with information security policies. Cultivating an information security culture however is a challenge for organisations, as differences in cultural values can lead to cultural contradictions. Cultural contradictions can in turn lead to conflict, which has an undesirable influence on employee compliance behaviour. The purpose of this research is to explain the nature of the relationship between emergent cultural contradictions in organisations and the information security compliance behaviour of employees.

Methodology: Structuration Theory was used as a theoretical lens to explain how cultural contradictions are implicated in employee compliance behaviour. The research methodology was qualitative in nature, comprising a case study with interviews as the data collection instrument. The qualitative data was analysed using thematic analysis to report on cultural orientations, emerging cultural contradictions, and a structural analysis on how cultural contradictions influence employee compliance with information security policies.

Findings: Cultural contradictions between the espoused values of employees and the security values underpinning technology, priorities, processes, and vision are shown to have an adverse effect on employee compliance with information security policies. Structural analysis also revealed that an ineffective security training programme can lead to an unintended consequence of non-compliance to information security policies. Furthermore, misaligned information security goals can result in employees circumventing information security policies, if they are deemed to conflict with their professional goals, which are further exacerbated by weakly enforced sanctions. Findings also show that power relations enacted within a multinational organisation can have an undesirable effect on the information security policy compliance behaviour of implementors and employees alike.

Value: The implications of cultural contradictions on employee compliance behaviour have received little attention in research. The few studies that have addressed the phenomenon have predominantly relied on value-based organisational theories. This study seeks to address this limitation by proposing a theoretical framework grounded in social theory, to explain how cultural contradictions are implicated in information security compliance behaviour.

Contents

1	Introduction.....	1
1.1	Background	1
1.2	Problem Statement	2
1.3	Research Question and Research Objective.....	3
2	Literature Review.....	4
2.1	Information Security Policy and Compliance Behaviour	4
2.2	Culture.....	5
2.3	Organisational Culture	8
2.4	Information Security Culture	11
2.5	Cultural Heterogeneity	12
2.6	Cultural Contradictions and Conflict	13
2.7	Summary	13
3	Theoretical Framework.....	15
3.1	The Use of Theory in this Study	15
3.2	Structuration Theory	17
3.3	Structure	18
3.4	Dimensions of the Duality of Structure.....	20
3.4.1	Signification.....	21
3.4.2	Legitimation.....	22
3.4.3	Domination	23
3.5	Structuration and Culture	24
3.5.1	Organisational Culture	25
3.6	Structuration Theory in IS.....	26
3.7	Structuration Theory and Cultural Contradictions	29
3.7.1	Contradictions	31
3.8	Structuration Theory and Information Security Policies.....	32
3.9	Key Concepts of Structuration Theory and Culture Summary	33
4	Research Methodology	38
4.1	Research Philosophy	38
4.1.1	Ontology	38
4.1.2	Epistemology	39

4.2	Research Approach	40
4.3	Research Strategy	40
4.3.1	Case Selection	41
4.3.1	Population and Sampling	41
4.4	Time Frame	41
4.5	Data Collection Instrument	42
4.6	Data Collected	43
4.7	Data Analysis	44
4.8	Ethical Considerations and Confidentially	47
4.9	Summary	47
5	Analysis and Findings	49
5.1	Case Description	49
5.2	Information Security Compliance Behaviour	49
5.2.1	Information Security Training	50
5.2.2	The Information Security Compliance Behaviour Level	51
5.3	Analysis of Culture	52
5.3.1	Rule Orientation	53
5.3.2	Goal Orientation	54
5.3.3	Support Orientation	56
5.3.4	Innovation Orientation	57
5.3.5	Information Security Culture	58
5.4	Cultural Contradictions	60
5.4.1	Priority Contradictions	60
5.4.2	Process Contradictions	62
5.4.3	Technology Contradictions	63
5.4.4	Vision Contradictions	65
5.4.5	Conflict and Non-Compliant Behaviour	67
5.5	Structurational Analysis	69
5.5.1	Information Security and Structures of Signification	70
5.5.2	Information Security and Structures of Domination	73
5.5.3	Information Security and Structures of Legitimation	86
5.5.4	Reflexive Monitoring and Change	91

5.6	Summary	97
6	Discussion and Theoretical Elaboration	99
6.1	Cultural Contradictions and Compliance Behaviour	99
6.2	Enacted Structures of Information Security Compliance Behaviour	102
6.2.1	Information Security Training and Compliance Behaviour.....	103
6.2.2	Information Security Goals and Compliance Behaviour	108
6.2.3	Information Security Sanctions and Compliance Behaviour	111
6.2.4	Information Security Policies and Compliance Behaviour - Perspective of Implementers and Employees	117
7	Conclusions.....	127
7.1	Theoretical Implications.....	128
7.2	Practical Implications	129
7.3	Limitations	131
7.4	Recommendations for Future Research	131
8	References.....	132
	Appendix A. Interview Guide.....	154
	Appendix B. Management Consent Form	156
	Appendix C. Individual Consent Form.....	158
	Appendix D. Ethics Approval Request.....	160
	Appendix E. Approved Ethics Application	161
	Appendix F. Sample Intranet Communication of Cultural Values.....	162
	Appendix G. Structures of Signification Themes	164
	Appendix H. Structures of Domination Themes.....	166
	Appendix I. Structures of Legitimation Themes.....	167

List of Tables

Table 1. Key Theoretical Concepts.....	33
Table 2. Interview Participants	43
Table 3. Six phases of Thematic Analysis (Braun & Clarke, 2006)	46
Table 4. Research Methodology Summary.....	47
Table 5. Security Awareness Simulations.....	50
Table 6. Phishing Simulation Report	52
Table 7. Employee Views of Power and Sanctions Data Extracts.....	75
Table 8. Contradictions Among Information Security Personnel.....	84
Table 9. Themes of Negative Interpretive Schemes of Information Security.....	95
Table 10. Cultural Contradictions Implicated in Compliance Behaviour	100
Table 11. Cultural Contradictions Implicated in Enacted Structures of Compliance Behaviour.....	124

List of Figures

Figure 1. Levels of Culture (Adapted from Karahanna et al., 2005)	7
Figure 2. The Theory Selection Process Followed (Adapted from Ononiwu et al., 2018)	17
Figure 3. Dimensions of Duality of Structure (Giddens, 1984).....	20
Figure 4. The Competing Values Framework (Adapted from Quinn, et al., 1999).....	26
Figure 5. Structuration Theory Model of IS-Mediated Compliance Behaviour	37
Figure 6. Employee Views of Power and Sanctions.....	75
Figure 7. Themes Associated with Negative Perceptions of Information Security	96
Figure 8. Information Security Training and Compliance Behaviour	105
Figure 9. Information Security Goals and Compliance Behaviour.....	109
Figure 10. Information Security Sanctions and Compliance Behaviour	113
Figure 11. Information Security Policies and Compliance Behaviour of Implementers	119
Figure 12. Information Security Policies and Compliance Behaviour of Employees	122

List of Abbreviations

Abbreviation	Definition
CIO	Chief Information Officer
HR	Human Resources
HSEQ	Health Safety Environmental and Quality
IAM	Identity Access Management
IS	Information Systems
ISP	Information Security Policy
ISPs	Information Security Policies
IT	Information Technology
PIM	Privileged Access Management
POPIA	Protection of Personal Information Act
SAP	Systems Analysis Program Development
VPN	Virtual Private Network

1 Introduction

1.1 Background

Many organisations today consider their informational assets to be critical to their business continuity, and therefore share concerns about their safeguarding (Trang & Brendel, 2019; Kappelman, et al., 2021). As a result, in 2018 alone organisations spent in excess of \$100 billion on securing information assets (Gartner, 2018), which was forecast to increase to approximately \$150 billion in 2022 (Gartner, 2021). One way of addressing information security concerns is through information security technology. However, as researchers and practitioners have shown, focusing exclusively on technology without considering how humans interact with systems is inadequate and could render information security technology ineffective (Chen, et al., 2021). A greater emphasis should be placed on human interactions with technology, as employees are generally regarded as the first line of defence in their interaction with others and information assets (Karlsson M. , Karlsson, Åström, & Denk, 2022).

Given the acutely human aspect of information security, it is important to investigate socio-cultural influences on information security compliance behaviour. Culture is shown to have a significant influence on an individual's information security behaviour (Solomon & Brown, 2021). This is partly because there is a correlation between an individual's espoused cultural beliefs and their ensuing compliance behaviour (AlHogail, 2015; Wiley, McCormac, & Calic, 2020). This notion is further affirmed by researchers who advance the idea of fostering a subculture of information security, where compliance to security policies becomes second nature (Da Veiga, Astakhova, Botha, & Herselman, 2020).

Recent reports indicate that the number of security incidents originating from the non-compliant behaviour of employees have either remained the same or increased (PricewaterhouseCoopers, 2018). This suggests that organisations have found it challenging to cultivate an effective information security culture in practice. It is argued that this is partly due to a discrepancy between academia and industry in their understanding of how to instil an information security culture (Da Veiga et al., 2020). In addition, the lack of consensus on a standard set of dimensions (Nasir, Arshah, Hamid, & Fahmy, 2019), as well as inconsistency in scales for assessing information security cultures (Orehek & Petrič, 2020), does not bode

well for practice. This study however agrees with Kolkowska (2011), that the problem is partly due to information security researchers generally assuming a view that culture is constant with little variation (Kolkowska, 2011). But culture is not homogenous and consists of various subcultures (Walsham, 2002). This implies that a “one size fits all” approach to information security culture is unlikely to be effective.

The heterogenous nature of culture implies that various subcultures could coexist in a dominant culture (Karahanna, Evaristo, & Srite, 2005). With varying subcultures come differing cultural values and norms (Da Veiga & Martins, 2017), which could lead to cultural contradictions and conflict, that ultimately influence information security compliance behaviour of employees. However, diverging cultural values could also compel employees to deepen their understanding of cultural contradictions, and thereby accommodate cultural difference to the benefit of the organisation. There is a lack of research addressing the influence of cultural contradictions on information security compliance behaviour (Kolkowska, 2011; Yayla & Lei, 2018). A study within the context of information systems (IS) development project performance, highlighted how the complexities of varying cultural contexts raised accompanying contradictions at various cultural levels (Geeling, Brown, & Weimann, 2020). Differing subcultures, as experienced by employees in the process of compliance behaviour, and the contradictions and potential conflict that follow needs further investigation. This study proposes to contribute to research and practice in this respect.

1.2 Problem Statement

Despite its benefits, organisations find it challenging to cultivate an effective information security culture and non-compliance behaviour continues to prevail (PricewaterhouseCoopers, 2018). The inability to create an information security culture is partly due to researchers assuming a uniform view of culture, rarely considering how different subcultures are implicated in information security compliance behaviour (Kolkowska, 2011). Different subcultures with diverging values and norms usually coexist within a given organisational culture (Da Veiga & Martins, 2017). Furthermore, cultural contradictions are found to emerge due to different cultural values and norms, potentially leading to cultural conflict (Walsham, 2002), which has implications on information security compliance behaviour. The influence of cultural contradictions and ensuing conflict on compliance behaviour is not well understood and has received little attention from

information security researchers (Dhillon, Syed, & Pedron, 2016; Karlsson, Denk, & Åström, 2018). The few studies that have addressed the phenomenon have predominantly relied on values-based organisational theories, which has limitations when studying cultural contradictions and conflict (Walsham, 2002). This reveals a need for supplementary approaches to studying the influence of cultural contradictions on information security compliance behaviour (Karlsson, et al., 2015; Yayla & Lei, 2018). This study proposes to address this research gap by obtaining data which will aid in understanding the cultural implications on information security compliance behaviour. The purpose of this research is therefore to explain the nature of the relationship between emergent cultural contradictions in organisations and the information security compliance behaviour of employees.

1.3 Research Question and Research Objective

The following research questions will be answered to address the research problem at hand.

Primary Research Question (RQ): RQ1: *How are cultural contradictions in organisations influencing the information security compliance behaviour of employees?*

Secondary research question:

- RQ2: What is the level of information security compliance behaviour with information security policies within a multi-national organisation?
- RQ3: What are the cultural contradictions that emerge in the process of information security compliance behaviour of employees?

This study consists of six key sections. The first section established the background of the problem at hand, including the research purpose, research questions and objectives. The second section covers a comprehensive literature review, culminating in a proposed theoretical framework for this study. The third section is a discussion of the research methodology that was followed. The fourth section deliberates over analysis results and findings. The fifth section entails a theoretical elaboration and discussion of research findings. The last section concludes with research implications, limitations, and recommendations for future research.

2 Literature Review

2.1 Information Security Policy and Compliance Behaviour

Organisations commonly use information security policies (ISPs) to define their information security standards and set the boundaries for technology usage (Cram, Proudfoot, & D'Arcy, 2017). ISPs are meant to complement information security technology, and provide employees with rules and guidelines for acceptable behaviour for the protection of information assets (Guo, Yuan, Archer, & Connelly, 2011; Yayla & Lei, 2018). While compliance to ISPs is necessary for effective information security management (D'Arcy & Teh, 2019), researchers have identified employee non-compliant behaviour as a significant challenge for organisations (Vance, Siponen, & Straub, 2020). To this end, security researchers and industry practitioners alike have invested time and effort to understand the antecedents of ISP compliance and non-compliance behaviour (Haeussinger & Kranz, 2017; Cram, D'Arcy, & Proudfoot, 2019). One of the most oft-used theories to explain employee behaviour is the Theory of Planned Behaviour (TPB) (Ajzen, 1991). The TPB posits that attitudes towards a behaviour, subjective norms, and perceived behavioural control influence intentions to perform a certain behaviour, which in turn mediates the actual behaviour (Ajzen, 1991). Information security research has tended to focus on intention as a predictor for compliance or non-compliance behaviour (Lowry, Dinev, & Willison, 2017).

Additionally, security researchers and practitioners have widely used General Deterrence Theory and deterrence methods, such as formal sanctions, to prevent behavioural intentions to violate ISPs (Ifinedo, 2014; Vance, Siponen, & Straub, 2020). Researchers however question the overreliance on sanctions as a means of altering intentions of non-compliance behaviour (Hedström et al., 2011). Guo et al. (2011) for example found that sanctions in the form of ISPs had no significant influence on an employee's intention to comply. Evidence also suggests that the formation of an organisational culture that respects policies might be a stronger motivator for security compliance behaviour (Hu et al., 2012). Information security researchers have therefore investigated how culture can be used to change employee behaviour, which will be discussed in the following section.

2.2 Culture

Historically, the concept of culture has its origins in the field of anthropology, where there is no real consensus on its meaning (Straub, Loch, Evaristo, Karahanna, & Srite, 2002). The term “culture” has been proven difficult to define. It is often used symbolically as a placeholder for various concepts that are equally difficult to define, such as social systems, social structures, institutions, environments, values, beliefs, and practices which direct human behaviour (Markus & Kitayama, 2010). According to Kroeber and Kluckholm (1952), the word “culture” is derived from the Latin verb *colere*, which means to tend or cultivate, and has traditionally been used interchangeably with the word “civilisation”. However, “civilisation” essentially refers to the “chain of variable but accumulative progress” (Kluckholm, 1952, p. 17) of humans and is often restricted to meaning advanced or high cultures. Similarly, the modern ethnographic use of the word “culture” refers to more than mere societal progress, but to a state or condition, often organic in nature, shared by humans in social organisation. The modern meaning of the term culture emanates from the German word “*Cultur*”, which refers to an organic state, shared by societies, that manifests in customs and beliefs (Kroeber & Kluckhohn, 1952). Linton (1945), in emphasising the social organisation of culture, defines culture as “the configuration of learned behaviour and results of behaviour whose component elements are shared and transmitted by the members of a particular society” (Linton, 1945, p. 32). This implies a reciprocal relationship between culture and agents. While culture influences human behaviour, the actions of agents reinforce or change that culture (Mironenko & Sorokin, 2018).

There has subsequently been a multiplicity of definitions of culture, which are often incoherent. Kroeber and Kluckholm (1952) for example, reviewed 164 different definitions of culture found in extant literature. Likewise, Smith (2016) reviewed definitions published in over 210 journal papers, books and chapters, and found them to be valuable, but incoherent when analysed collectively. He argues that the plurality of incoherent definitions is partly due to the failure of researchers to explicitly state and agree on their ontological assumptions. This leads to a weak ontological consensus and thus forgoes a clear foundation upon which all the diverse conceptualisations of culture can be synthesised to form an agreed upon definition (Jahoda, 2012). Likewise, there has been a lack of consensus among IS researchers on the definition and meaning of the term culture (Straub et al., 2002; Tams, 2013), as IS researchers tend to glean off the works found in other fields, such as anthropology and

sociology in this case. While the plurality of definitions allows for richness and a multifaceted view of sociocultural behaviour, it can also result in vagueness, ambiguity and incoherence as to its meaning (Smith, 2016). This makes it difficult for researchers to understand its core meaning and grasp what culture “is” as opposed to what culture “has” and what it can “do”.

While some (Smith, 2016) detest the seeming incoherence, others argue that the many definitions are indicative of the malleable nature of culture as a social construct, and attempts to find a single definition are futile (Jahoda, 2012). Hence, instead of attempting to find the one unified definition, researchers have instead attempted to categorise the various definitions. For example, Jahoda (2012) categorised definitions arbitrarily into three groups, namely 1) conceptualising culture as external, 2) as internal or external, or both, and 3) groupings of several definitions. More pertinent to the field of IS, and more relevant to this study, is Straub et al.’s (2002) categorisation of definitions into three groups within the field of IS, namely defining culture as shared values, as a problem-solving device, or as a creation of the mind and a way of being.

Definitions based on shared values and meanings are the most oft-used conceptualisation of culture within extant literature (Alvesson, 2002; Gelfand, Nishii, & Raver, 2006; Leidner, 2010; Smith, 2016), where values are recognised as an essential distinguishing characteristic of culture (Kroeber & Kluckholm, 1952; Karahanna et al., 2005). A similar bias is observed within IS literature, where culture is largely examined as cultural values and their unidirectional impact on technology outcomes (Leidner & Kayworth, 2006). According to Karahanna et al. (2005, p. 5), “Values refer to relationships among abstract categories that are characterised by strong affective components and imply a preference for a certain type of action”. Meglino and Ravlin (1998), citing Rokeach (1973), describe two types of values as either embedded in objects, or as held by individuals. Values however are not only shared but also shaped by culture (Roccas & Sagiv, 2010).

According to Walsham (2002), a prevailing theoretical example of approaching culture as shared values in IS literature is Hofstede’s dimensions for national culture (Hofstede, 2011). Hofstede’s work is valuable as it allows researchers to assign a cultural value, or dimension, to a group based on geographical boundaries, and thus allows for intercultural comparisons between groups. Hofstede’s dimensions have been heavily relied upon in Information Systems studies at the level of national culture (Leidner, 2010). This conceptualisation

however does not account for the fact that cultures and subcultures could span across multiple geographical boundaries (Straub et al., 2002). Hofstede et al. (2010) admits that individuals are generally members of multiple incongruent cultural groups which could lead to conflict. Walsham (2002) notes that while Hofstede provides a valuable mechanism for understanding cultural differences, he provides no analytical tools to study the conflict that could arise from intercultural differences.

Extant literature shows that several subcultures can coexist within an organisation (Da Veiga & Martins, 2017). Researchers have therefore examined compliance behaviour at various cultural levels of analysis. Emphasising one level of analysis however could oversimplify cultural complexity and misrepresent the effects of culture on an individual's actions (Yammarino & Dansereau, 2011). To this end, Karahanna et al. (2005) conceptualised the overlapping cultural levels which could influence an individual's behaviour. As depicted in Figure 1, compliance behaviour can be influenced by a multitude of cultural levels (Solomon & Brown, 2021).

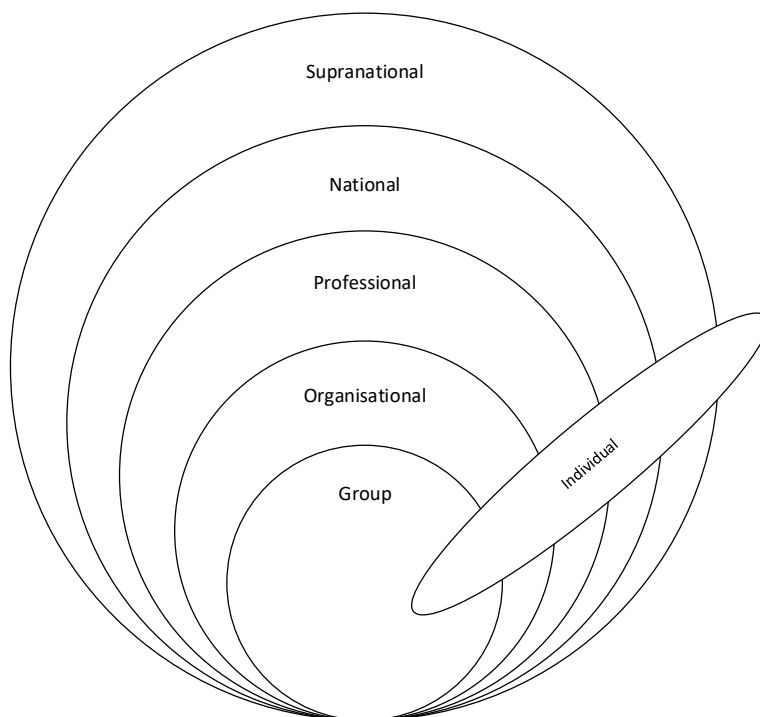


Figure 1. Levels of Culture (Adapted from Karahanna et al., 2005)

2.3 Organisational Culture

The research discipline of organisational culture has its foundations in the field of anthropology and organisational climate research (Van Muijen, et al., 1999), and suffers the same definitional fate as found in its roots (Alvesson, 2002). Smircich (1983) pointed out that organisational theories are largely predicated on different ontological assumptions stemming from the ongoing debate between objectivism and subjectivism. The former views social reality as grounded in objective features, such as structures, as opposed to being anchored in the minds and consciousness of social actors as with the latter (Alvesson, 2002). Furthermore, assumptions about human nature, such as determinism and voluntarism, dictate how researchers approach the concept of organisational culture. Determinism views culture as having an asymmetrical, and often unidirectional, power relationship with individuals. With voluntarism, culture is an enactment of social actors where humans possess the power to produce culture. Both approaches tend to be unidirectional in their view of the relationship between social systems, such as culture, and individuals. This ontological dualism between objectivism and subjectivism is largely addressed by what Weaver and Gioia (1994) called second-order multi-paradigm views, such as Structuration Theory, as proposed by Giddens (Giddens, 1984). As a meta-theory, Structuration Theory offers dualities, as opposed to dichotomous paradigms, where the relationship between social structures, such as culture, and human agency are viewed as inseparable and reciprocal (Walsham, 2002). Structuration Theory is therefore a possible solution to this ontological dilemma when studying organisational culture and can be considered if the researcher seeks to embrace the benefits of both objectivism and subjectivism (Orlikowski, 1992; Jones & Karsten, 2008).

Smircich (1983), in reviewing classical concepts of organisational culture, highlighted the two distinguishing approaches of conceptualising culture as either a variable or as a root metaphor. Researchers who approach organisational culture as a variable tend to be more objectivist in their ontological assumptions, where social reality is considered to be objective and grounded in observable structures, and other objective features of an organisation (Alvesson, 2002). In this view, culture is something an organisation has, and can be known by observing relationship patterns within an organisation (Smircich, 1983). This is of particular interest to comparative management studies, where predictability and establishing causality are deemed important in order to achieve organisational control. Research within this perspective often follow quantitative research methods (Schneider, Ehrhart, & Macey,

2013). Furthermore, conceptualising culture as shared values and beliefs provides organisational members with a sense of identity, facilitates commitment to the organisation, enhances social stability, and serves as a sense-making device to members (Smircich, 1983). Culture is therefore seen as an instrument and a means of control for management (Alvesson, 2002). This is not dissimilar to Straub et al.'s (2002) categorisation of viewing culture as a problem-solving device.

In contrast to treating culture as a variable, researchers approaching culture as a root metaphor emphasise the idea that an organisation itself should be understood as a culture. That is, culture is not something an organisation “has”, but culture is what an organisation “is”. Culture as a root-metaphor goes beyond an instrumental view of understanding organisations and advances the view of “organizations as expressive forms, manifestations of human consciousness” (Smircich, 1983, p. 347). Proponents of this view of organisational culture tend to follow an inductive method of inquiry as it allows the researcher to analyse the experiences of organisational members (Schneider et al., 2013). Methodologically, researchers advocating this view favour qualitative methods, as it allows the researcher to observe the unique expressions and manifestations of organisational culture.

Another difference between the two approaches is their views on how social systems, and culture, is produced and reproduced (Alvesson, 2002). Researchers advocating a variable approach to culture which highlights predictability tend to adopt a deterministic view of culture (Myers & Tan, 2002), and thus social structure and agency. That is, culture as a social system determines the behaviour of organisational members. Organisational culture in this view is treated as static, linear and unidirectional, allowing for predictability in analysis (Schultz & Hatch, 1996).

Proponents advancing the idea of culture as a root-metaphor tend to maintain an autonomous view of human agency in relation to culture (Alvesson, 2002). Instead of viewing organisational culture as a determining force on human behaviour, agents are seen as autonomous with the capacity to choose otherwise (Giddens, 1984). That is, through their interactions, agents are in an ongoing process of producing and reproducing culture. The difference between the two perspectives is then in the view that culture either creates individuals or individuals create culture (Alvesson, 2002). This is essentially a dichotomy between determinism and autonomy.

An oft-used model for organisational culture within the field of information security is Schein's (2010) cultural layers (Karlsson et al., 2015; Nasir et al., 2019). Schein defined culture as "a pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration" (Schein, 2010, p. 17). Schein identified three layers of organisational culture, namely artefacts, values and underlying assumptions. Values in Schein's definition refer to adopted ideologies and beliefs, while artefacts refer to any observable item, such as newsletters, language or websites. The third and deepest layer of underlying assumptions refers to the deep-rooted behaviours of individuals.

Studies examining national culture and IS are largely influenced by Hofstede's (2011) six-dimensional framework (Myers & Tan, 2002; Walsham, 2002). The six values being Power Distance, Uncertainty Avoidance, Individualism-Collectivism, Masculinity-Femininity, Long Term-Short Term Orientation and Indulgence-Restraint. Likewise, information security researchers have relied heavily on Hofstede's work when studying cultural influences on security outcomes within organisations (Karlsson et al., 2015).

Yet another influential model for organisational culture is Quinn's (1988) Competing Values Framework (CVF), which depicts four essential orientations of organisational culture. The four orientations are Clan Cultures (which are internally focused and emphasise flexibility), Adhocracy Cultures (which are externally focused and emphasise flexibility), Hierarchical Cultures (which are internally focused and emphasise control) and Market Cultures (which are externally focused and emphasise control).

All three of the aforementioned commonly used theorisations of organisational culture in IS literature, focus primarily on identifying distinguishing values shared by a group or culture (Leidner & Kayworth, 2006; Jackson, 2011; Kolkowska, 2011; Karlsson et al., 2015). This is largely because there is a correlation between espoused cultural values of employees, and their ensuing behaviour, and compliance behaviour (Wiley, et al., 2020). Furthermore, values have an intuitive appeal in studying cultures as they are a well-used construct that evidently lend themselves to being measured (Morris, et al., 1998).

2.4 Information Security Culture

The effectuality of information security is ultimately dependant on an organisation's capability to cultivate an information security culture, where employee compliance to ISPs is a norm (D'Arcy & Teh, 2019). Information security culture is commonly defined as the values, attitudes and assumptions towards information security which are shared among employees within the organisation (Da Veiga & Elof, 2010). This definition is largely deduced from Schein's (2010) three cultural layers, which is the most widely used cultural model within information security research (Karlsson et al., 2015). Following a comprehensive literature review of differing definitions, Da Veiga et al. (2020) defined information security culture as "contextualised to the behaviour of humans in an organisational context to protect information processed by the organisation through compliance with the ISP and procedures and an understanding of how to implement requirements in a cautious and attentive manner as embedded through regular communication, awareness, training and education initiatives." (Da Veiga, et al., 2020, p. 19).

It is worth noting the difference between an information security culture and a cyber security culture. While information security is contextualised to the cultivation of a culture within the confines of an organisation, cyber security culture has a societal context instead (Reid & Van Niekerk, 2014). This distinct difference is because information security entails the protection of information in general, while cyber security involves the protection of information in cyber space in particular (von Solms & von Solms, 2018). Given the nature of this study's research strategy, the scope of the case study is limited to the concept of information security culture.

The most widely accepted theorisations of information security culture in information security literature focus primarily on the shared values. The two most influential cultural frameworks of Schein's (2010) and Hofstede's (2011) both share the view that culture is manifested in shared values and norms (Walsham, 2002; Kolkowska, 2011; Karlsson et al., 2015). Researchers however have questioned the explanatory power of values in grasping cultural differences. The inconclusive empirical results of value-based studies cast doubt on whether values can fully explain cultural differences (Gelfand, Nishii, & Raver, 2006). In addition, attributing values exclusively at a group level implies that values are unanimously adopted by all group members, making it difficult to explain cultural differences within groups (Leidner & Kayworth, 2006). So, while the use of values has aided our understanding

of cultural difference, there has been an increased call for new approaches to supplement this contribution and go beyond the limitations of aggregated dimensions (Myers & Tan, 2002; Gelfand et al., 2006). This study proposes to contribute in this regard by providing novel insights on the cultural implications on information security compliance behaviour.

2.5 Cultural Heterogeneity

The predominant conceptualisation of culture with the IS discipline is the conceptualisation of consistency and uniformity in cultural values (Leidner & Kayworth, 2006). This is indicative of the dominance of values-based cultural theories, such as those put forward by Hofstede and Schein. Walsham (2002) labelled this prevalence as “Hofstede-Type Studies”, which makes little provision for an analysis of the effects of cultural heterogeneity. Hence, cultural studies within the IS discipline have been criticised for espousing a homogenous view of culture, where the values held by individuals in a culture are uniform (Straub, et al., 2002).

Similarly, information security culture studies typically favour a static view of culture as the values-based theories of Hofstede and Schein dominate research (Solomon & Brown, 2021). Considering the saturation of such “Hofstede-Type Studies”, Karlsson et al. (2015) recommend adopting theories from disciplines other than organisational science. This study will therefore adopt Structuration Theory (Giddens, 1984) from the field of sociology as a sensitising lens for analysing the cultural aspects of the information security compliance behaviour.

Still, the idea of shared values and norms alludes to a degree of homogeneity and systemness within a culture. In this regard, Structuration Theory has the potential to help analyse shared aspects, while implicitly holding in tension the concept of heterogeneity (Giddens, 1984). A structural analysis allows for examining the differing degrees of homogeneity within a heterogenous culture. Walsham (2002) points out that Structuration Theory can allow for a level of cultural analysis which goes down to subgroups and even individuals, thus making Structuration Theory ideal for studying cultural contradictions and conflict within a heterogenous culture.

2.6 Cultural Contradictions and Conflict

Cultural contradictions emerge as a result of divergent values, norms and practices held by individuals and groups. Geeling, Brown, and Weimann (2020) show that cultural contradictions, arising from different overlapping levels of culture, could have an adverse effect on the efficiency and effectiveness of social interaction in IS development projects. If contradictions are the main fault lines for potential conflict, then conflict is the actual activity of struggle between individuals or groups (Walsham, 2002).

Within the field of information security, the effects of cultural contradictions and resulting conflict are largely under-studied (Karlsson et al., 2018). Hedström et al. (2011) studied the effects of value conflict on information security compliance behaviour and found professional values to take precedence over information security values, which leads to non-compliant behaviour. Kolkowska (2011) found that several value conflicts emerge between departments, which stifles the formation of an information security culture. While providing valuable insights into cultural value conflict and information security compliance behaviour, these studies all espouse a values-based approach to the phenomenon, which has its limitations (Karlsson et al., 2015).

2.7 Summary

Information security technology and ISPs are necessary for organisations to protect their information assets. An aim of ISPs is to define information security standards and guide employee compliance behaviour (Cram, et al., 2017; Yayla & Lei, 2018). Even with robust information security technology and well-defined ISPs, employee compliance behaviour remains the weakest link in information security systems (Wiley, et al., 2020). Employee non-compliance behaviour is found to be a significant challenge for organisations (Vance, et al., 2020). Thus, Researchers have proposed cultivating a culture of information security, where ISP compliance is second nature (D'Arcy & Teh, 2019). Cultivating an information security culture however is a challenge as organisations generally have multiple subcultures with competing values and norms, which can ultimately lead to cultural contradictions and conflict (Walsham, 2002). Cultural value conflict is found to lead to information security non-compliance behaviour (Hedström, et al., 2011; Kolkowska, 2011). The influence of cultural contradictions and conflict on employee compliance behaviour are largely understudied (Karlsson et al., 2018). Furthermore, there is an overreliance on values-based

organisational theories when studying information security culture (Hedström et al., 2011; Kolkowska, 2011; Yayla & Lei, 2018). While contributing significantly to information security culture research, values-based theories has its limitations when studying cultural contradictions and conflict (Karlsson et al., 2015).

The following section discusses the limitations of values-based theories in studying cultural contradictions, and also explicates the grounds for selecting Structuration Theory as a theoretical guide for empirical analysis.

3 Theoretical Framework

A theory can be defined as an abstract statement of relationships between concepts that helps us understand the real world (Bacharach, 1989; Varpio, Paradis, Uijtdehaage, & Young, 2020). A comprehensive theory typically contains elements answering questions of “what”, “how”, and “why” (Whetten, 1989). Theories are generally typified based on their level of generalisation as either meta-theories, mid-range theories, or substantive theories (Gregor, 2006). Meta-theories, such as Structuration Theory (Giddens, 1984), are highly abstract and provide grand generalisations about social patterns. Mid-range theories, such as the CVP (Van Muijen, et al., 1999), are moderately abstract with limited scope, addressing specific aspects of human interaction. Substantiative theories, such as typified cultural contradictions that could emerge in information systems development (Geeling, Brown, & Weimann, 2020), address more specific areas of inquiry. The level of generalisation of a theory is indicative of its scope and breadth of applicability (Saunders, Lewis, & Thornhill, 2012).

Following is a discussion on how theory was used and selected in this study.

3.1 The Use of Theory in this Study

Gregory (2006), in a taxonomy of theory types, identified five distinct *causa finalis*, the final cause, inherent in each theory, namely analysis, explanation, prediction, explanation and prediction, and design and action. This study, by using Structuration Theory as its sensitising lens, will use theory primarily to provide explanations of what a phenomenon is, and how and why it happens (Gregor, 2006; Lee, 2010). In addition, theory can be used to guide the research design and data collection, inform the iterative data collection and analysis process, or as the eventual outcome of research (Walsham, 2002). The use of theory in this study encompasses all three usages.

Saunders et al. (2012) point out that while a deductive approach to reasoning moves from theory to data, and inductive reasoning moves from data to theory, abductive reasoning on the other hand moves to-and-fro between theory and data. In abductive reasoning a preliminary theoretical framework is usually adopted which consists of articulated preconceptions (Dubois & Gadde, 2002). As research activity moves back and forth between theory and empirical observations, the understanding of both theory and data are expanded. This developed understanding might uncover the need to redirect or reframe the initial theoretical

framework through expansion or change (Kovac & Spens, 2005). The activity of reframing the theoretical framework is an iterative process, often requiring a search for additional theories, which Dubois and Gadde (2002) call theory matching or systematic combining. This implies that the theoretical context can be changed or expanded during research, hence Walsham (2006) posited that theory can be used in a “lighter or tighter” (Walsham, 2006, p. 324) manner. Similarly, this study employed abductive reasoning starting with a prior theoretical framework, and through the iterative process of analysis, unveiled theoretical preconceptions which required expansion.

Furthermore, it is shown that appropriate theories can be selected at various stages of the research process (Ononiwu, Brown, & Carlsson, 2018). This study followed Ononiwu et al.’s (2018) model for background theory selection, as depicted in Figure 2. Walsham’s (2002) adaptation of Structuration Theory was used as the preliminary background theory, which informed the research design phase. Bernardi’s (2017) conceptualisation was then selected as an additional theory after the iterative phase of analysis. The justification for theory selection during each phase and key concepts is delineated in the following two sections.

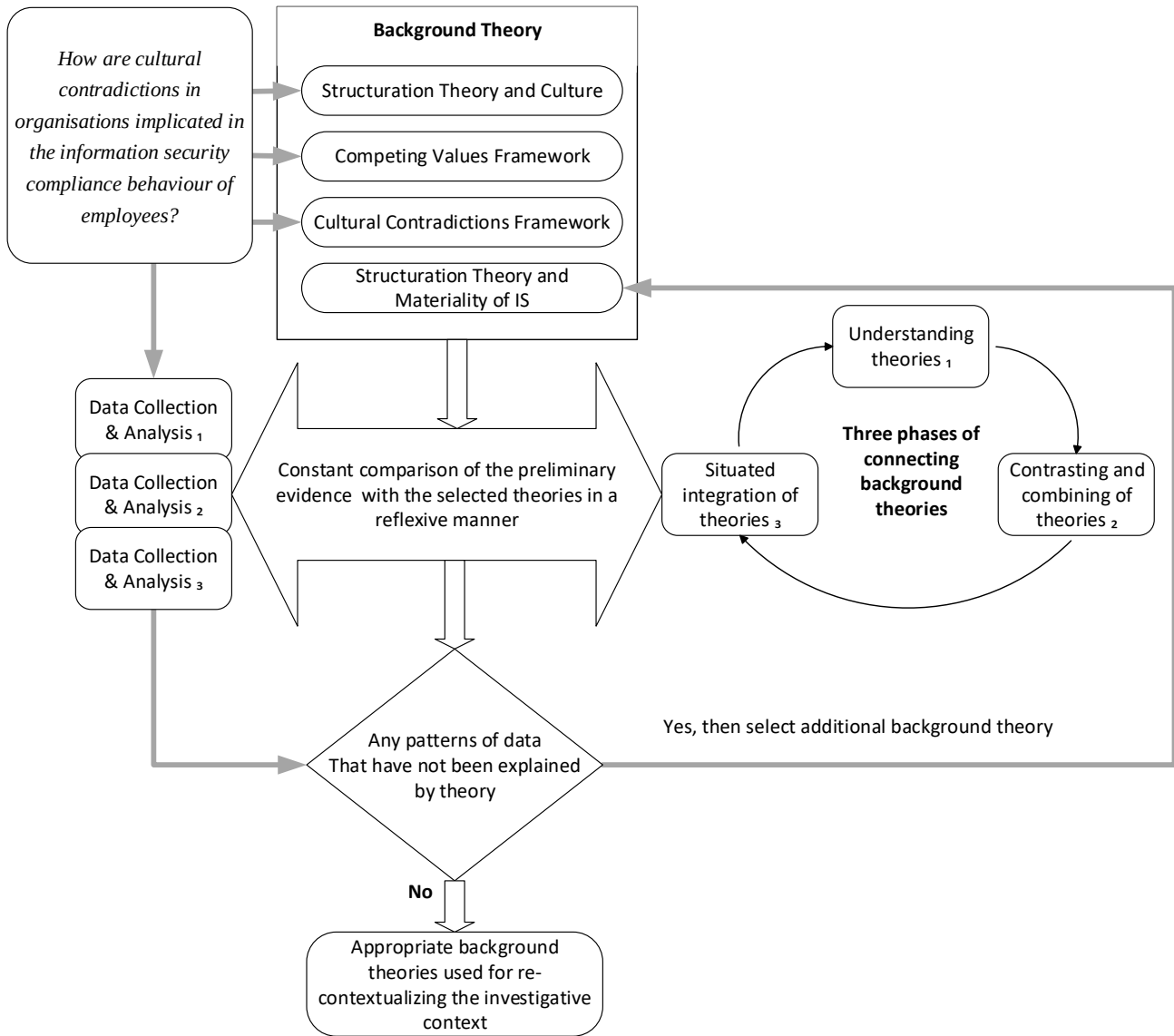


Figure 2. The Theory Selection Process Followed (Adapted from Ononiwu et al., 2018)

3.2 Structuration Theory

Structuration Theory was selected as the interpretive lens for this study, firstly due to its treatment of contradictions and conflict, allowing the researchers to comprehensively analyse cultural contradictions and conflict (Walsham, 2002). Secondly, previous studies have observed an overreliance on organisational/management theories in information security research and recommend the use of complementary social theories instead (Karlsson et al., 2015).

Structuration Theory makes a distinction between contradictions and conflict, making it possible to not only identify contradictions but also analyse how these contradictions could lead to conflict (Giddens, 1984). By using Structuration Theory as its sensitising lens, this study will heed the call of Karlsson et al. (2015) for deeper insights into information security culture, which supplement value-based organisational theories. It is also in keeping with Myers and Tan's (2002) suggestion to go beyond the concept of simplistic national cultural values within IS research. Following is a discussion of the key concepts that constitute Structuration Theory.

3.3 Structure

Structure can be regarded as the rules and resources which exist within the human mind as structural properties of social systems (Jones & Karsten, 2008). In other words, "structure can be seen as rules of behaviour and the ability to deploy resources, which exist in the human mind itself, rather than as outside constraints" (Walsham, 2002, p. 361). Individuals will draw upon these rules and resources in their social behaviour, while at the same time recursively producing and reproducing structures, which comprise rules and resources. Giddens (1984) also made a distinction between structure and structures in its plural meaning. While structure refers to rules and resources recursively implicated in social practice, structures refer to rule-resource sets underlying the observable conditions for social system reproduction (Giddens, 1984).

Rules refer to the generalisable routines and procedures enacted in the production and reproduction of social practices (Jones, Orlikowski, & Munir, 2004). Giddens (1979) distinguished between two aspects of rules that are implicated in social routines and practices, namely rules relating to the "constitution of meaning, and that relating to sanctions involved in social conduct" (Giddens, 1979, p. 82). Put another way, "social rules have both constitutive and regulative (sanctioning) aspects to them" (Giddens, 1979, p. 66). The former refers to aspects of rules as it relates to the constitution of meaning or codes of signification, while the latter refers to right and wrong conduct or codes of legitimation (Giddens, 1984). For example, in the former instance, to understand the expression "locking my computer", it is important to understand what the term "locking" means. It could entail using physical hardware, such as a lock and key, or it could mean using software of some kind. In an example of the latter instance of rules, locking my computer may be desirable but sharing the

key or password with a stranger is deemed unacceptable conduct which could lead to sanctions. The latter aspect relates to rules as implicated in correct norms and acceptable modes of conduct when “locking my computer”. Defined this way, rules are essentially principles of behaviour which exist in the mind of actors (Walsham, 2002).

Rules can be formulated as verbal expressions or codified (Giddens, 1984), such as formal ISPs. Inappropriate conduct which violates codified information security rules and policies could effectively lead to sanctions and punishment. The aspects of rules and sanctioned conduct are shown to be significant in shaping information security compliance behaviour (Siponen & Vance, 2010; Tang, Li, & Zhang, 2016). Furthermore, sanctions and penalties are also widely used as a method of deterring behaviour which violates ISPs (Siponen & Vance, 2010; Ifinedo, 2014). Organisations can draw upon rules of meaning and conduct when applying sanctioning penalties for security policy violations (Arhin & Wiredu, 2018). The two aspects of rules essentially constitute structures of signification and legitimation respectively.

Resources as a structural property refer to the ability to deploy authoritative and allocative resources (Pozzebon & Pinsonneault, 2005). Giddens (1984) distinguished between two types of resources, namely authoritative and allocative resources. Authoritative resources refer to the capability to exercise command over human resources, while allocative refers to the capability to exercise command over objects or material (Giddens, 1979). Refining the conceptualisation of allocative resources, Sewel (1992) argued that allocative resources, if material as posited by Giddens, should be actual as opposed to virtual. Previous studies also argue that IS as a resource can be viewed as containing institutional properties, which structures the actions of social actors as they use technology over time and space (Walsham & Han, 1990; Orlikowski, 2000). Thus, Walsham (2002) postulated that IS embody rules of meaning, norms and resources.

Building on these studies and on Sewel’s reconceptualization of allocative resources, Bernardi (2017) theorises the material features of health IS as defining the “rules and norms implicated in the reproduction of social practices” (Bernardi, 2017, p. 935). An IS can therefore be viewed as an allocative resource, containing rules of meaning and norms (Walsham, 2002). Thus, although IS do not embody structure in structural terms, as it exists only as memory traces in the human mind, they are however implicated as rules and resources in recurring social practices, as actors interact with technology over time. This is

congruent with one understanding among researchers that IS often have cultural values, rules and norms embedded in them (Leidner & Kayworth, 2006; Koch, Gonzalez, & Leidner, 2011; Koch, Leidner, & Gonzalez, 2013). It is also proposed that information security and privacy, which can be viewed as abstract constructs, should be at the heart of IS research (Lowry, et al., 2017). Information security artefacts can therefore be conceptualised as allocative resources from a structuration perspective.

There is essentially an interplay between rules and resources, and the two cannot be separated in conceptualization (Giddens, 1984). Resources are “the modes whereby transformative relations are actually incorporated into the production and reproduction of social practices” (Giddens, 1984, p. 18).

3.4 Dimensions of the Duality of Structure

For analytical reasons, Giddens (1984) conceptualised three dimensions of structure, as depicted in Figure 3, namely signification, domination and legitimation (Giddens, 1984). Signification refers to rules or codes of meaning which exist as both the medium and outcome of communication in social interaction. Domination refers to the capacity to exercise power over authoritative and allocative resources, while legitimation refers to the sanctioning of legitimised conduct (Orlikowski, 1992; Bernardi, 2017).

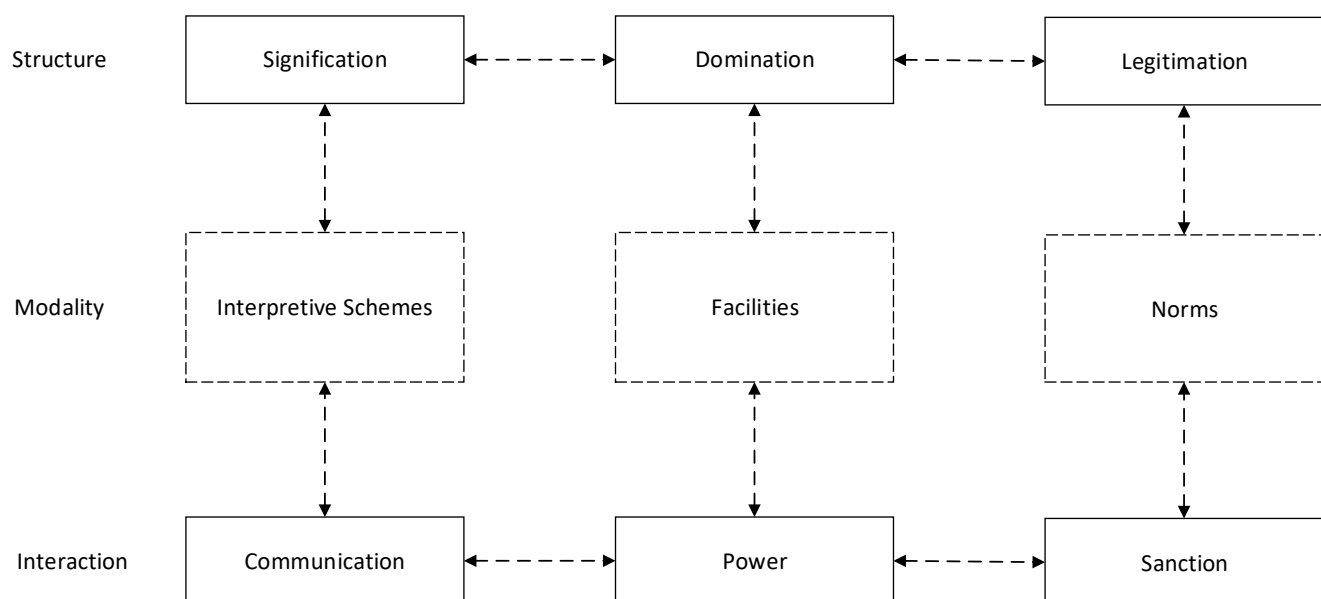


Figure 3. Dimensions of Duality of Structure (Giddens, 1984)

While structures of signification, domination and legitimation are the structural dimensions of a social system, the interactions of actors with social structures have the corresponding analytical dimensions of interaction, namely communication, power and sanctions (Jones & Karsten, 2008). Furthermore, the human interactions are interlinked with the dimensions of structure by three intermediary dimensions of structuration, which Giddens calls the “modalities of structuration” (Giddens, 1979, p. 81). The modalities of structuration are what agents draw upon in social interaction and constitute the core dimensions of the duality of structure, which is central to Structuration Theory (Giddens, 1979). While structure exists in the minds of human actors, modalities are the expressions of structural dimensions implicated in interaction (Whittington, 2015). The modalities which interlink structure with human interaction are interpretive schemes, facilities, and norms (Jones & Karsten, 2008).

3.4.1 Signification

The structural dimension of signification informs and is informed by the interpretive schemes of actors, which are the standardised stocks of knowledge reflexively applied in the communication of meaning (Giddens, 1984). Interpretive schemes “form the core of mutual knowledge whereby an accountable universe of meaning is sustained through and in interaction” (Giddens, 1979, p. 83). Agents draw upon interpretive schemes to make sense of the world around them (Walsham, 2011) in the “production and reproduction of interaction” (Giddens, 1984, p. 29). That is, through interpretive schemes, human actors in the communication of meaning either produce or reproduce structures of signification (Walsham & Han, 1990). Essential to the modality of interpretive schemes is the idea that human actors are knowledgeable about their social systems and apply that knowledge reflexively (Pozzebon & Pinsonneault, 2005). Knowledgeability refers to a human actor’s stocks of knowledge about the conditions of their day-to-day actions and of others (Giddens, 1984).

Structures of signification and the modality of interpretive schemes have relevance to both organisational culture and information security. Organisational culture itself is often conceptualised as containing shared interpretive schemes or cognitive structures, which employees draw upon to make sense of the collective world around them (Leidner & Kayworth, 2006). Knights and Willmott (1987) could therefore use aspects of Structuration Theory to show how organisational culture can be used as a management strategy to cultivate desired interpretive schemes for employees to draw upon (Alvesson, 2002). This is not

dissimilar to the idea of cultivating a security culture, where the protection of information and compliance with ISPs becomes part of the way things are done (Da Veiga, et al., 2020).

Knowledge of interpretive schemes are necessary for agents to act (Sewell, 1992). Similarly, the knowledgeability of employees about their day-to-day information security conditions are important in producing and reproducing a security culture (Van Niekerk & Von Solms, 2010). Researchers have subsequently examined the effects of knowledge-rich communication, with an emphasis on information security, on structures of signification and modes of interpretive schemes (Arhin & Wiredu, 2018). Furthermore, ISPs are interpretive schemes and cultural artefacts which are entrenched in an organisation's security values (Chen, Ramamurthy, & Wen, 2015; Lowry et al., 2017).

3.4.2 Legitimation

The structural dimension of legitimation is linked to interactive structures of sanctions by “modes of normative regulation, by which ‘legitimate orders’ are sustained” (Giddens, 1979, p. 97). Human agents draw upon the modality of norms in sanctioning their actions, thereby producing and reproducing structures of legitimation (Walsham, 2011). While this emphasises human agency, structures of legitimation also have a constraining influence on social actors. Institutional norms are essentially the rules governing appropriate or legitimate conduct within an organisation (Orlikowski, 1992). Structure is therefore both an enabling and a constraining influence on social actions. Organisations can exercise a constraining influence on human conduct by drawing on structures of legitimation in deploying sanctions against inappropriate conduct (Giddens, 1984; Arhin & Wiredu, 2018).

Norms are shared within a social system as structural properties, thus maintaining a degree of systemness (Giddens, 1984). According to Walsham (2002), this view is commensurate with the basic conception of culture as consisting of norms, shared by a collective. Norms are the institutional rules that govern legitimate conduct (Orlikowski, 1992), and which can be understood as the behavioural expectations of a collective (Pozzebon, 2004). According to Cram et al. (2019), there is direct association between social norms and the security behaviour that ensues. Information security researchers have therefore historically relied on theories which are partly predicated on the idea that an individual's behaviour is influenced by subjective norms (Ifinedo, 2014; Yazdanmehr & Wang, 2016; Safa, Von Solms, & Furnell, 2016), such as proposed by Ajzen (1991) in the Theory of Planned Behaviour.

Organisations can draw upon structures of legitimation in order to aptly apply sanctions and punishment for security violations (Arhin & Wiredu, 2018).

ISPs (as “modes of normative regulation”, i.e., norms) contribute to structures of legitimation because they inherently include the sanctioning of appropriate security conduct and the associated penalties for policy violations. Arhin and Wiredu (2018) therefore argue that organisations can draw upon structures of legitimation in order to aptly apply sanctions when employees violate ISPs. Information security researchers have also historically emphasised using the certainty and severity of sanctions as a means of deterring noncompliance to ISPs (Siponen & Vance, 2010; Bulgurcu, Cavusoglu, & Benbasat, 2010; Yayla & Lei, 2018).

In addition, the structural dimension of legitimation must be understood in conjunction with structures of signification, as well as structures of domination, as they are inextricably linked in reality and separable only analytically (Giddens, 1984). In fact, Giddens (1984) argues that the concept of accountability is a clear expression of the juncture between interpretive schemes and norms. That is, actors draw upon interpretive schemes to explain and account for their actions as well as provide normative grounds for their justification. In Giddens’s terms, accountability refers to the “accounts that actors are able to offer of their conduct draw upon the same stocks of knowledge as are drawn upon in the very production and reproduction of their action” (Giddens, 1979, p. 57). Bernardi (2017), in using Structuration Theory to study accountability in health IS, argues that structures of signification, legitimation and domination together hold social actors accountable for their actions by ensuring acceptable conduct.

3.4.3 Domination

The institutional property of domination is dependent on the ability of actors to draw on facilities in interaction, such as exercising power over allocative and authoritative resources. Allocative resources refer to the transformative capacity to exercise power over material objects, while authoritative resources involve exerting command over people (Whitman & Mattord, 2012). Structures of domination are what actors draw upon in the exercising of power over allocative and authoritative resources (Indeje & Zheng, 2010). Allocative resources refer to material objects, while authoritative resources involve people (Whitman & Mattord, 2012). Resources, via interpretive schemes in signification and normative regulations in legitimation, are a means through which power is exercised (Giddens, 1984).

Power in Structuration Theory is not to be understood as a form of constraint or determinism, where structures of domination reproduce docile actors. Power in Structuration Theory is a two-way relationship which involves both autonomy and dependence in social interactions (Giddens, 1984). Giddens (1979) refers to this as the dialectic of control, where subordinates have the potential to influence their superiors, and thus change structures of domination (Orlikowski, 1992). For example, Walsham (2002) found a subtle resistance to the implementation of a new information system. Instead of overtly rejecting the new information system, staff expressed a form of passive resistance by electing not to use it at all. Thus, subordinates could exercise a degree of control over their superiors by the way they manage resources.

Power understood this way also has information security implications. Human actors, by drawing on their stocks of knowledge and through the dialectic of control, can choose how they respond to organisational rules (Sewell, 1992). That is, social actors have the power to choose their behavioural response to ISPs, and thereby reproduce or produce structures of signification, legitimation and domination. While this perspective emphasises an agency vantage point, power is a two-way relationship between structure and agency (Giddens, 1984). From an institutional perspective, power is exercised by an organisation's management by implementing ISPs to constrain employee behaviour, with the aim of reproducing desired structures (Arhin & Wiredu, 2018).

3.5 Structuration and Culture

The process of structuration is “the production and reproduction of social systems through the application of generative rules and resources” (Riley, 1983, p. 415). In analysis, structuration is the observable conditions which govern the transformation of social structures, and thereby the reproduction of social systems (Giddens, 1984). In other words, structuration is, as Giddens put it in referencing Derrida, “the structuring of structure” (Giddens, 1979, p. 61).

Similarly, culture theorists posit a ceaseless interaction between social actors and culture to produce and reproduce cultural values (Kroeber & Kluckhohn, 1952). On this basis, Kissack and Callahan (2010) contend that the process of meaning-making in culture is analogous to the process of structuration. In fact, earlier research applying Structuration Theory to the field of accounting, conceptualised the process of structuration as producing and reproducing a given culture (Boland, 1985). It is further argued that organisational culture theory, applied

within IS research, can be comfortably contained with the meta-framework of Structuration Theory (Robey, 1995).

3.5.1 Organisational Culture

Organisational culture itself is posited as an institutional phenomenon within structuration theory, thus containing structural features that are recursively enacted (Riley, 1983). This ongoing enactment, stabilised over time and space, becomes institutional features that are exhibited as the structural properties of a social system (Giddens, 1984). Thus, structure, exhibited as structural properties, such as is found in culture (Riley, 1983), exists only in its instantiations and in the minds of human actors.

Walsham (2002) conceptualises culture at its most basic form as shared symbols, norms and values, and positions culture as containing the “systems of meaning, forms of power relations, and sets of norms” of a collective (Walsham, 2002, p. 362). Thus, culture contains the structural properties as expressed in rules and resources. While rules and resources may exist in the mind of individuals, they also contain enough “systemness” to be viewed as shared in a social collective, such as a given culture (Giddens, 1984). Walsham (2002) was therefore able to use the concept of systemness in structural properties to extrapolate contradictions and conflict to cross-cultural work in IS.

The CVF was selected as the theoretical basis for investigating the general cultural orientation of an organisation and its different subcultures (Cameron & Quinn, 2011). The need to systematically complement social structural analysis with insights into salient cultural values, was a primary motivation for choosing the CVF as the theoretical lens for scrutinising organisational culture. Theory selection on the premise that it will give meaningful insights into a phenomenon is deemed a valid reason for choosing a theory (Walsham, 2006). Furthermore, the CVF partly informed the data collection phase of this study (Schutt, 2012). In addition, the CVF models cultural value orientations as conflicting or competing within an organisational culture (Quinn, Hildebrandt, Rogers, & Thompson, 1991), making it a fitting lens for analysing an organisation’s culture (Ngwenyama & Nielsen, 2003).

The CVF depicts the cultural orientations of Rules, Goals, Support and Innovation as four quadrants across two primary value dimensions, as illustrated in Figure 4 (Faerman & Quinn, 1985; Quinn et al., 1991; Cameron & Quinn, 2011). Rule-oriented cultures focus on internal processes that facilitate stability and control. Goal-oriented cultures focus on their external

environment and maintain control by setting goals for employees to achieve (Quinn et al., 1991). Support-oriented cultures are internally focused with a flexible orientation in their structures (Faerman & Quinn, 1985). Innovation-oriented cultures are externally focussed with a strong emphasis on flexibility (Quinn & Rohrbaugh, 1983).

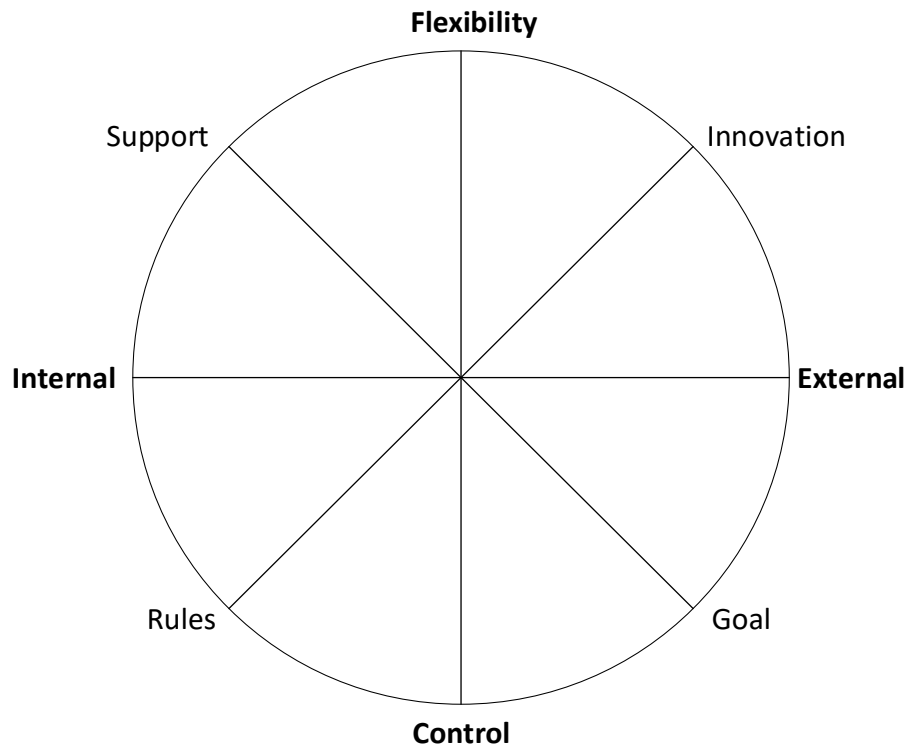


Figure 4. The Competing Values Framework (Adapted from Quinn, et al., 1999)

An important consideration in this study’s examination of culture is the notion of cultural heterogeneity. Culture is not a static set of values espoused by all members of a group, but instead is dynamic and heterogeneous (Myers & Tan, 2002; Markus & Kitayama, 2010). Although this could make culture an elusive concept to define, it does however help in this study to remain cognisant of cultural differences in analysis.

3.6 Structuration Theory in IS

Giddens (1984) made no explicit treatment of technology within his theory of structuration. In the particularisation of Structuration Theory, IS researchers largely agree that Gidden’s notion of structure as a virtual order implies that perceiving technology as embodying social structure can be problematic (Jones et al., 2004; Jones & Karsten, 2008). Instead, in accordance with Gidden’s conception of structures as existing “only in their instantiation” (Giddens, 1984, p. 304), IS are only implicated as rules and resources in recurring social

practices when actors use elements of technology over time (Orlikowski, 2000). Technology can therefore be viewed as providing the space for potential human action (Jones & Karsten, 2008). Furthermore, it is also argued that actors often draw upon IS in their interaction with technology over time to provide a sense of meaning, power and legitimization (Walsham, 2002). Structuration Theory has subsequently become an influential theoretical paradigm within IS research (Poole & DeSanctis, 2002; Jones & Karsten, 2008). Within IS it is largely used to understand the interactions between human agents and technology, and how their intended and unintended consequences are implicated within organisations (Bernardi, 2017).

Jones and Karsten (2008) note that the use of Structuration Theory within IS research can be categorised into three streams, namely, the application of structural concepts, the application and development of an IS-specific version, and the critical engagement with Structuration Theory. In the first stream, researchers largely accept Structuration Theory in general and seek to apply all or some of its concepts. For example, Walsham (2002) applied Structuration Theory in general to study the impact of cross-cultural working on IS projects. Similarly, aspects of Structuration Theory were used to explain how organisational culture influences Integrated Financial Management Information System projects (Indeje & Zheng, 2010). The theory has also been applied in the development of an IS Framework to aid the issuing of identity documents to citizens (Mutudi & Iyamu, 2020). Others used elements of Structuration Theory to understand the implementation of IS in the primary healthcare industry (Kouroubali, 2002; Jeffries, et al., 2017). Additionally, Orlikowski's (2000) conceptualisation of Structuration Theory has been applied in an analysis of E-Commerce adoption within a developing country (Kabanda & Brown, 2017). Most IS research falls within the first stream in the way they use Structuration Theory (Jones & Karsten, 2008).

The second stream addresses the perceived weaknesses of Structuration Theory by developing an IS specific version (Jones & Karsten, 2008). One perceived weakness is Giddens's apparent lack of explicit treatment of IS (Walsham, 2002). In addressing this weakness, three noteworthy contributions within the second category are DeSanctis and Poole's (1994) Adaptive Structuration Theory (AST), Orlikowski's (2000) practice lens for studying technology, and Bernardi's (2017) adaptation of the materiality of technology in the process of structuration. Firstly, Poole and DeSanctis (2002) argued that Structuration Theory gives a limited consideration for technology and therefore developed an Adaptive Structuration Theory (AST). A key proposition of AST is that social structures are

incorporated and embedded within technology at the time of design (DeSanctis & Poole, 1994). Technology is therefore seen as a source of structures, consisting of rules and resources, which can incite change in social structures (Poole & DeSanctis, 2002). However, the idea that technology embodies structure can be problematic as it is a departure from Giddens's original view of structure as a virtual order, instantiated only in social practices (Orlikowski, 2000; Jones et al., 2004). Furthermore, AST appears to emphasise explaining behavioural variances and predictive outcomes (Poole & DeSanctis, 2002). Hence, it is noted that most applications of AST in research tend to adopt a variance approach, through dependent and independent variables, to determine cause and effect (Pozzebon & Pinsonneault, 2005). This form of soft determinism in seeking regularities, it is argued, bears little resemblance to Giddens's original theory of structuration (Rose, 1998; Orlikowski, 2000; Pozzebon & Pinsonneault, 2001; Jones & Karsten, 2008). As Walsham (1990) points out, the variability of human beings, and human action, makes any form of soft determinism infeasible.

The second noteworthy contribution in this category, and in addressing the perceived limitation, is Orlikowski's (2000) practice lens for studying technology, which reconceptualises the role of technology in the process of structuration. Orlikowski's (2000) conceptualisation essentially extends Giddens's (1984) perspective on technology, by proposing a practice lens for understanding of the ongoing interactions between humans and technology, and the implications on social structures. Orlikowski (2000) rejects the notion that technology embodies structure and returns instead to Giddens's (1984) original assertion that structure is only instantiated in practice. Thus, using a practice lens, technology-in-practice focuses on emerging structures as human actors use technology. That is, technology-in-practice refers to "the particular structures of technology use that users enact when engaging recurrently with a technology" (Orlikowski, 2000, p. 411).

A third noteworthy contribution is Bernardi's (2017) conceptualisation of the materiality of technology. Bernardi's (2017) theorising is partly premised on the works of Sewel (1992) and Orlikowski (1992). Sewel (1992) argued that allocative resources, according to Giddens's (1984) definition, are actual instead of virtual. Orlikowski (1992) in her earlier work also adopted the notion of interpretive flexibility of technology. The interpretive flexibility of technology refers to the extent to which human actors are involved in the physical and social constitution of technology during its development and in use (Orlikowski, 1992). Bernardi

(2017), building on the work of Sewel (1992) and Orlikowski (1992), and in addressing a perceived weakness in Structuration Theory, used the notion of interpretive flexibility to account for the materiality of health IS. On the one hand, the material features of technology are shaped by actors during development and use. On the other hand, the material features of technology, defined by rules and norms, also sets the boundaries and limits how users interpret and use technology. There is therefore a mutual shaping relationship between the technology domain and the social domain. Bernardi (2017) showed how material features embedded in technology can “shape the rules, norms, and meanings implicated in the reproduction of social structures that legitimize accountability” (Bernardi, 2017, p. 947).

Research within the last stream of critical engagement explores the limitation of the theory. Research within this category highlights the strengths and weaknesses in comparison to other theories. For example, critical realists argue that ontologically social reality does not exist solely in the mind of actors, and material conditions could influence social actors directly (Archer, 1995).

Of interest to this study is Walsham’s (2002) application of Structuration Theory in studying cross-cultural environments and IS. By using Structuration Theory, the study provided a deeper analysis of the cultural contradictions and conflict that emerge within a heterogenous cultural environment (Jones & Karsten, 2008). This is due to Giddens’s (1984) considerations for contradictions and conflict that might emerge in social interactions, which makes it ideal for answering the research question at hand.

In addition, this study adopts Bernardi’s (2017) view of materiality, that technology contains virtual qualities in the form of rules, norms, and authoritative resources, while it also contains actual material qualities in allocative resources. ISPs, whether formally codified or embedded in IS, are therefore conceptualised as encompassing rules, norms, and resources within this study.

3.7 Structuration Theory and Cultural Contradictions

An element of Structuration Theory which is key to this study is its treatment of structural contradiction and conflict. Social systems exhibit structure through structural properties, which “are both medium and outcome of the practices they recursively organize” (Giddens, 1984, p. 25). Structural properties are presented as institutional features, stretched over time

and space which, although real, exist only in the instantiations of social reproduction practices (Pozzebon & Pinsonneault, 2005). The structural properties that are most deeply embedded and implicated across space and time are structural principles (Giddens, 1984). Structural principles are the principles of organising societies to produce identifiable clusters of institutions. That is to say, structural principles are the clustering of interconnected and transformative relations which govern the reproduction of social systems (Giddens, 1979). Differences in structural principles which governs system reproduction in an organisation, emerge as contradictions (Walsham & Han, 1990).

According to Giddens (1984), the identification of distinct structural principles and structural properties facilitate a comprehensive analysis of institutions, and specifically of culture (Walsham, 2002). By identifying clusters of structural principles, researchers can differentiate between sets of structures which are contradictory within an organisation (Riley, 1983). Through modalities, human agents can draw on multiple structures in their interactions, which leads to sets of structures either mediating or contradicting one another (McPhee, Poole, & Iverson, 2016). These mediating or contradictory structures become evident as structures are produced and reproduced through structural principles. The idea of structural principles makes Structuration Theory ideal for analysing social structures for contradictions in institutional analysis.

Structuration Theory also makes a distinction between structural contradictions and conflict. While contradiction may arise from opposing structural principles, conflict on the other hand is the actual struggle which stems from contradictions between individuals or groups (Giddens, 1984). Structural contradiction therefore has the potential for conflict, if opposing structural principles affect actors negatively. Alternatively, social actors could experience structural contradiction as non-threatening, and compromise by acting in the common interest of both structural principles. An important consideration to this distinction is the idea of knowledgeable actors who can choose their own action. During actual conflict or struggle, knowledgeable actors still have the power and ability to act on their own principles (Walsham, 2002). Giddens (1979) therefore argues that while contradiction is a structural concept, linked to domination, conflict on the other hand is linked to the interactive structure of power and is experienced in practice. That means social actors can either act on their own structural principles in interaction when contradictions arise, which can lead to conflict, or they can seek to compromise and potentially act upon the common interest of both structures.

Over time, individuals can learn to compromise and take actions to address cultural conflict (Walsham, 2002). This is similar to the Processes of Relating in information systems development, as posited by Geeling et al. (2017), which is the process of understanding contradictions and accommodating cultural differences. Thus, a coordinated culture is produced, or as Brannen and Salk (2000) termed it, a negotiated culture, where a compromise is reached between different groups. This illustrates the dynamic nature of culture, as both coordinated and negotiated cultures contain existing cultural elements as well as new and opposing cultural elements. In analysing similar cross-cultural working in a software production environment, Walsham (2002) maintains that a structural analysis of cultural contradictions and conflict provides a fitting theoretical framework to ground such analysis.

3.7.1 Contradictions

This research will rely on a particularisation of Geeling et al.'s (2020) illustration of various forms of cultural contradictions within IS development. Their research identified the relative occurrences of Priority Contradictions, Process Contradictions, Role Contradictions, Technology Contradictions, and Vision Contradictions as a result of cultural differences. Vision Contradictions refer to the misalignment of goals between individuals and groups. Priority Contradictions can be defined as the mismatching value systems which inform how individuals and groups prioritise aspects of IS development projects (Geeling, et al., 2020). Process Contradictions refer to the differences in day-to-day work practices as a result of different cultural values held between groups or individuals. Role Contradictions occur as a result of different beliefs regarding associated responsibilities. Technology Contradictions occur when there is a difference between embedded values within IS artefacts and what is expected from users. These forms of contradictions may apply equally to information security, as security objectives are often in conflict with business or personal objectives (Van Niekerk & Von Solms, 2010). For example, organisational goals which contradict personal goals are found to give rise to conflict between parties, which has an adverse effect on ISP compliance (Karlsson, Hedström, & Goldkuhl, 2017; Chen, Li, Chen, & Yin, 2021). Similarly, information security is often in contradiction with the efficiency of IS, which conflicts with business processes and the daily tasks of employees (Hwang, Kim, Kim, & Kim, 2017; Xu & Guo, 2019).

3.8 Structuration Theory and Information Security Policies

A review was conducted of information security literature to establish the extent to which Structuration Theory was used, firstly to study information security behaviour, and secondly to study cultural contradictions and conflict. The resulting publications examined various facets of information security behaviour, none of which were cultural contradictions and conflict. The results also indicate that most information security literature employing Structuration Theory falls within the first research stream, as categorised by Jones and Karsten (2008). That is, the application of Structuration Theory to understand the relationship between IS and organisations. For example, one such study proposed using Structuration Theory as a theoretical basis for studying the strategic alignment of information security management (Kovács *et al.*, 2017). Another study used the theory to explore the intended and unintended consequences of security awareness programmes on organisational structures (Tsohou, Karyda, Kokolakis, & Kiountouzis, 2015). Andersson *et al.* (2022) used a structurational analysis to uncover the enactment of structures in information security standard development, and the legitimacy claims of those standards.

ISPs contribute to both structures of signification, domination, and legitimation. They contribute to interpretive schemes as they set the organisation's security standards and define the compliance behaviour that is expected of employees (Cram *et al.*, 2017). Structures of signification inform, and are informed by, the interpretive schemes which employees draw on as they make sense of their own information security actions and that of their peers (Andersson, Hedström, & Karlsson, 2022). The power that management possesses to define and implement ISPs, with the goal of guiding employee compliance behaviour, is an example of the enactment of structures of domination (Arhin & Wiredu, 2018). In addition, structures of domination are implicated as information security personnel draw upon their own skills and expertise to influence the development and implementation of ISPs (Andersson *et al.*, 2022). Furthermore, IS, with their embedded security features, can be conceptualised as allocative resources in structures of domination (Bernardi, 2017). IS with associated ISPs both shape and are mutually shaped by facilities, norms, and interpretive schemes in social interaction. ISPs also embody modes of normative regulations *i.e.*, norms, as the organisation can draw upon legitimation structures in sanctioning information security compliance behaviour, and thereby hold employees accountable for their actions (AlHogail, 2015; Arhin & Wiredu, 2018). Andersson *et al.* (2022) also show how legitimation structures are enacted

in the development of information security standards, as actors rationalise legitimacy for standard development actions.

To our knowledge, a structurational analysis of cultural contradictions and conflict in information security research is yet to be conducted. Information security researchers who have addressed cultural contradictions and conflict, have largely used values-based culture theories to analyse differences in cultural values (Hedström et al., 2011; Kolkowska, 2011; Yayla & Lei, 2018). While providing valuable insights, value-based approaches to studying cultural contradictions makes little provision for cultural heterogeneity in analysis (Walsham, 2002).

3.9 Key Concepts of Structuration Theory and Culture Summary

A summary of the key concepts of Structuration Theory, culture and information security in this study is illustrated in Table 1. Structure is a virtual order which exists as memory traces in the minds of human agents (Giddens, 1984). Structure consists of rules of behaviour and the ability to deploy resources. The information security actions of an individual will draw upon these rules and resources, thereby producing or reproducing structures in the mind of the actor.

Table 1. Key Theoretical Concepts (Adapted from Giddens, 1984; Cameron & Quinn, 1999; Walsham, 2002; Bernardi, 2017; Geeling et. al., 2020)

Theoretical Concepts		Reference
Structuration Theory and Materiality	Structure:	
	Structure as a virtual order which exists as memory traces in the human mind.	Giddens, 1984
	The three dimensions of structure are signification, domination, and legitimation.	Giddens, 1984
	Modalities:	
	The three dimensions linking action and structure are interpretive schemes, facilities, and sets of norms.	Giddens, 1984

	• Information systems, with their embedded information security policies, embody interpretive schemes, provide resources (facilities), and encapsulate norms, and are deeply implicated in the modalities interlinking action and structure. • Information systems, with their embedded information security policies, are allocative resources in the technology domain, and mutually shape the interpretive schemes, facilities, and norms of actors in the social domain. Reflexivity and Change: • Human beings reflexively monitor their own information security compliance behaviour and the compliance of others and observe consequences, creating a basis for social change.	Walsham, 2002 Bernardi, 2017 Walsham, 2002
Culture	• Culture is conceptualised as shared values, norms, and symbols in a social collective. • Meaning systems (interpretive schemes), power relations, behavioural norms exist not merely in the mind of one person, but often exhibit a degree of systemness to consider them being shared. • There is a need to recognise a variety of cultural levels influencing compliance behaviour. • Varying cultural layers have salient orientations towards rules, goals, support, and innovation. • Information security culture is the shared values, attitudes, and assumptions of a collective towards information security.	Walsham, 2002 Walsham, 2002 Walsham, 2002 Cameron & Quinn, 1999 Da Veiga & Eloff, 2010

Cross-cultural Contradictions and Conflict	• Conflict is the actual struggle between actors and groups. • Contradiction is the potential basis for conflict arising from divisions of interest in vision, priority, process, role, and technology between cultural levels. • Conflict may occur in cross-cultural working if differences affect actors negatively and if they are able to act, leading to non-compliance behaviour.	Giddens, 1984 Geeling et. al., 2020 Walsham, 2002
---	--	--

IS embody interpretive schemes, facilitate the deployment of resources, and incorporate normative actions (Walsham 2002). In addition, information systems are allocative resources which contain material features that define the interpretive schemes, and norms that are implicated in social practice reproduction (Bernardi, 2017).

Culture is commonly conceptualised as encapsulating the values, norms and symbols shared by a social collective (Hofstede, 1980; Schein, 1990). In structuration terms, while signification, domination, and legitimation structures may exist in the minds of individuals, they also possess enough “systemness” to be regarded as shared among a culture (Giddens, 1984). The structural properties of a social system can be used as an analytical device to identify intra-cultural diversity (Riley, 1983; Walsham, 2002).

According to Giddens (1984), contradictions can emerge due to differing structural principles, such as differences in cultural backgrounds. Structural principles are the principles of organisation within societies, by which clusters of institutions are produced and reproduced (Giddens, 1979). While contradictions may arise due to differences in structural principles, conflict is the actual struggle in social practices that ensues between different cultures. Contradictions therefore have the potential for conflict if a social actor is affected negatively by the cultural differences, which has an undesirable effect on compliance behaviour (Karlsson et al., 2018).

Additionally, Structuration Theory emphasises human knowledge and reflexivity in the duality of structure. Structures in the human mind could appear to be solely a determining force, dictating the behaviour of social actors. Giddens (1979) however asserts that human

agents are also knowledgeable beings, with a capacity to draw on their stocks of knowledge in social interaction. Human agents are knowledgeable beings with the innate ability to reflexively monitor their own actions, and the actions of others (Giddens, 1984). Human knowledgeability and reflexivity form the basis for social change (Walsham, 2002). Similarly, the information security knowledge of actors, and their ability to reflexively monitor their own information security behaviour, has information security implications. Through knowledgeability and reflexive monitoring human agents can monitor the intended and unintended consequences of their own security actions (Hsu, Backhouse, & Silva, 2014). If an employee reflexively monitors the consequences of their information security behaviour and deems it to be negative, then they will most likely act differently in future when presented with the same security conditions.

The systematic combining of key concepts drawn from Structuration Theory, the CVF, and the varying types of emerging contradictions, formed the basis for this study's initial theoretical framework (Van Muijen, et al., 1999; Walsham, 2002; Geeling, et al., 2020). Walsham (2002) incorporates a conceptualisation of culture, contradictions, and conflict in his adaptation, which makes it a fitting analytical lens in answering the secondary research question of the effects of cultural contradictions. The theoretical framework guided the research design and data collection phase and formed the basis for the preliminary data analysis.

The abductive process of constant comparison of empirical observations and the preliminary adaptation of Structuration Theory (Walsham, 2002), revealed an insufficient treatment of the material features of information security. Bernardi's (2017) adaptation accounts for the materiality of IS, and adequately illustrates the mutual shaping relationship between the technology domain and the social domain. IS, as an allocative resource with material features within the technology domain, have a mutual influence on the modalities of interpretive schemes, facilities, and norms within the social domain. Knowledgeable agents reflexively monitor the conditions and consequences of actions as they mobilise modalities in the technology domain and social domain, and effectively produce and reproduce structures. Bernardi's (2017) conceptualisation sufficiently explains the material features of information security, and was therefore integrated with the initial background theory to produce the synthesised theoretical framework, illustrated in Figure 5. Both adaptations focus their

analysis at the modality level of the structuration process, which makes them commensurate in theoretical elucidation.

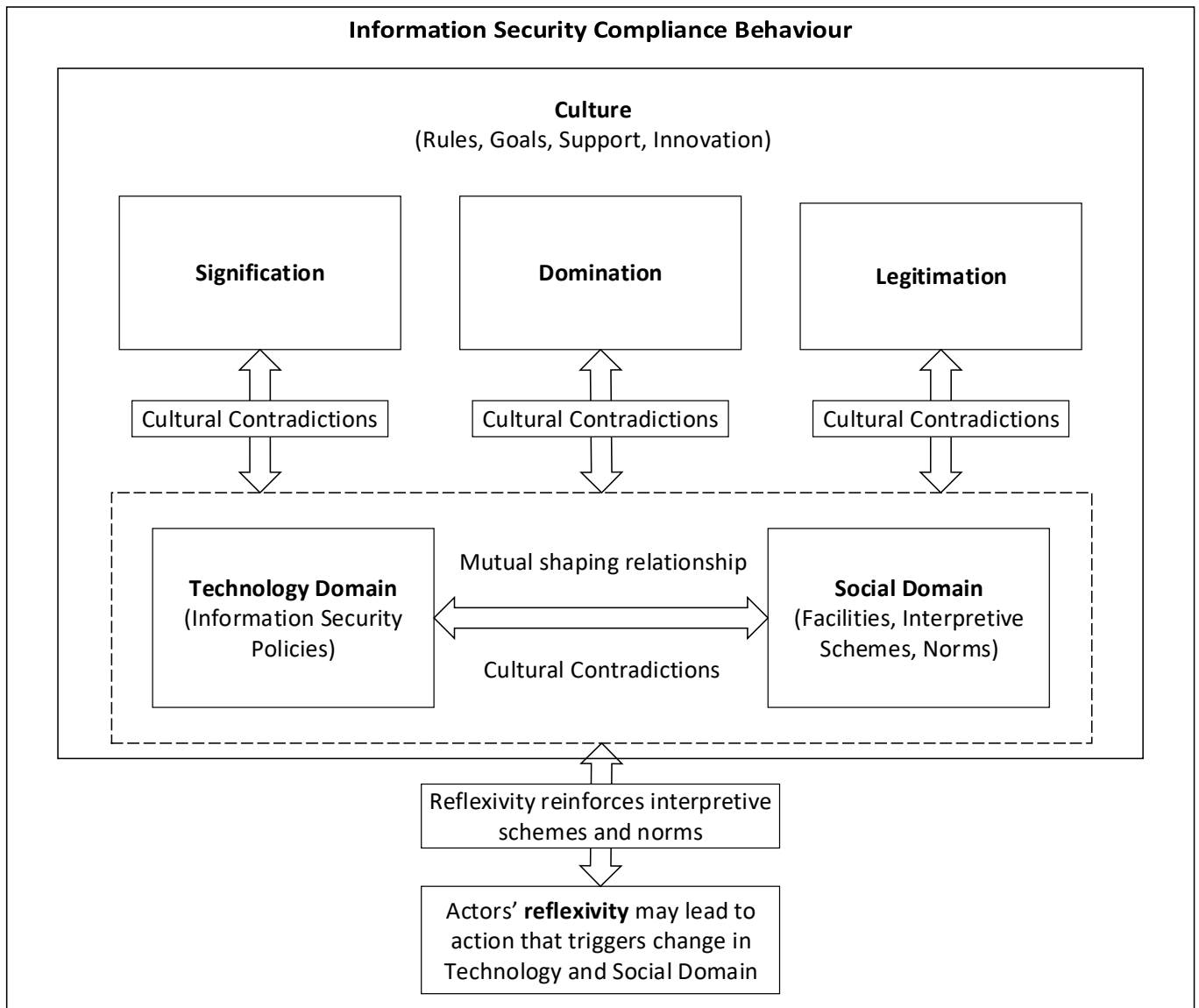


Figure 5. Structuration Theory Model of IS-Mediated Compliance Behaviour

4 Research Methodology

This section outlines the methodological approach used to answer the research question at hand. The first section discusses the ontological and epistemological assumptions, as well as the research approach underpinning the choice of research design. The next section delineates the research design to be adopted, followed by a discussion on the appropriate research methods to be followed, data collection and analysis techniques, ethical considerations, and research limitations.

4.1 Research Philosophy

Aspects regarding appropriate theory selection and suitable research methods are all considerations of a philosophical nature (Hassan, 2018). Thus, all researchers approach a phenomenon with a philosophical paradigm which governs their research. A philosophical paradigm is a set of ontological and epistemological assumptions which researchers use to frame and organise their reasoning (Schultz & Hatch, 1996; Bhattacharjee, 2012).

The proposed ontological and epistemological considerations held in this study will be discussed in the following two sections. The third section explains the appropriate research approach adopted.

4.1.1 Ontology

Ontology refers to a researcher's espoused assumptions about the nature of reality and social existence (Saunders et al., 2012). The two prevailing ontological positions held by researchers are objectivism and subjectivism. Objectivism views the social world as objective and independent of humans and can be comprehended objectively (Orlikowski & Baroudi, 1991). Subjectivism on the other hand views reality as socially constructed and within the minds of social actors (Bhattacharjee, 2012). The ontological assumptions of a researcher have an influence on the conceptualisation of organisational culture. Researchers adopting an objectivist stance tend to have an instrumental view of culture (Alvesson, 2002), where culture is seen as something an organisation "has" (Smircich, 1983). In this view organisational culture is treated as a variable which can be measured objectively, and which has a determining influence on its members (Myers & Tan, 2002). An objectivist ontological

approach is also most widely adopted among information security researchers (Dhillon & Backhouse, 2001; Cram et al., 2017).

Researchers adopting a subjectivist approach generally view organisational culture as a root-metaphor for an organisation, and as something an organisation “is” (Alvesson, 2002). In this view, organisational culture is seen as an expression and manifestation of the human mind (Smircich, 1983). Organisational members are seen as autonomous agents, who through their interactions produce and reproduce organisational culture, which is like the process of structuration. A subjectivist ontology is more consistent with Giddens’s (1984) Structuration Theory, which is the proposed theoretical framework guiding this study. This study therefore adopts the ontological stance that the social world is constructed by human actors through their interaction, and is thus subjective in nature (Orlikowski & Baroudi, 1991).

4.1.2 Epistemology

Epistemology refers to assumptions about how to construct and evaluate knowledge (Orlikowski & Baroudi, 1991). The epistemological assumptions of positivism and interpretivism are the two most common approaches taken by researchers (Saunders et al., 2012). Positivism in general holds that knowledge creation is limited to what can be observed and measured objectively, and therefore assumes an objectivist ontology (Bhattacharjee, 2012). Positivist research can also be qualitative, e.g., Pare (2004) describe how positivist qualitative case studies can be conducted with inductive reasoning.

Interpretivism commonly holds that individuals create their own subjective meanings about reality and assumes a subjectivist ontology (Orlikowski & Baroudi, 1991). Knowledge about reality can be obtained by understanding the meanings assigned by individuals (Bhattacharjee, 2012). An interpretivist approach therefore requires the researcher to enter the social world of social actors and conduct research among participants (Saunders et al., 2012). An interpretivist researcher effectively becomes the research instrument themselves (Weber, 2004).

This study will adopt an interpretivist epistemology as it is more closely aligned to the proposed structuration framing. Social structure, as posited by Structuration Theory, exists as memory traces in the mind of actors (Giddens, 1984), which makes interpretivism a fitting epistemology for this study.

4.2 Research Approach

There are three common research approaches to reasoning, namely deductive, inductive, and abductive. Although positivist inductive reasoning can be applied to case study research (Pare, 2004), deductive reasoning is typically associated with positivism, where the researcher postulates and tests a theoretical proposition (Saunders et al., 2012). With inductive reasoning, the researcher's goal is to infer theory from empirical data and is generally adopted for theory generation (Bhattacharjee, 2012). In abductive reasoning, the researcher proposes a hypothetical framework or frameworks, but not necessarily a priori, that could explain a phenomenon, and locates empirical data within a theoretical framework or frameworks (Mingers, Mutch, & Willcocks, 2013; Conlon et al., 2020). An abductive approach tends to result in theory refinement as opposed to theory generation (Dubois & Gadde, 2002). Peirce (1974) explained, "Deduction proves that something must be; Induction shows that something actually is; Abduction merely suggests that something may be" (Peirce, 1974, p. 106).

An abductive approach to reasoning has been identified as most suitable for this study. By proposing Structuration Theory as a sensitising lens, the researcher will start with a premise and generate testable conclusions from empirical data. The researcher will continuously move between the theoretical framework and the empirical data, which is consistent with abductive reasoning (Dubois & Gadde, 2002).

4.3 Research Strategy

The choice of research method depends on the type of research question to be addressed, the extent to which the research focus is on contemporary events, and the extent of control exercised over behavioural events (Rowley, 2002). The research question at hand seeks to explain *how* cultural contradictions are implicated in compliance behaviour. *How* questions, according to Rowley (2002), are best answered using a case study for empirical inquiry. Furthermore, a case study strategy is most appropriate for abductive studies (Dubois & Gadde, 2002). On this basis, a case study method was selected for this study.

4.3.1 Case Selection

Case studies can consist of one or multiple cases. A determining factor is whether the research problem requires comparisons to be drawn (Dubois & Gadde, 2002). This study's research question did not necessitate comparisons, which justified a single case study.

Case selection is important and must be determined by the research question, purpose, and theoretical background (Rowley, 2002). Case selection depends on whether the case is representative and situated across theoretical dimensions (Seawright & Gerring, 2008). The selected case is representative as multiple subcultures were represented, providing the necessary variation along the dimensions of theoretical interest (Seawright & Gerring, 2008).

Furthermore, Rowley (2002) point out three constraining factors which contribute to case selection - (1) the organisation and participants must be accessible, (2) resources must be available, and (3) within time constraints. The selected case for this study was accessible, and within both resource and time constraints. It represented a large organisation within the energy industry. The organisation had well established ISPs and awareness programmes, with established social structures which included multiple layers of culture.

4.3.1 Population and Sampling

Defining the population from which the research sample is drawn is important as it demarcates the boundaries for generalisation (Eisenhardt, 1989). Purposive sampling was used (Keutel, Michalik, & Richter, 2014). The participants were selected from management, information security, technical, enterprise architecture, auditing, retail, and service operations roles. Thus, potentially representing multiple subcultures and situated across the theoretical dimension. The aim was to interview 18 participants from varying departments who interact with IS daily.

4.4 Time Frame

Research designs are commonly either cross-sectional or longitudinal. The former entails collecting data at a point in time, providing a snapshot of a phenomenon (Orlikowski & Baroudi, 1991). The latter entails collecting data at two or more points in time, where the researcher engages with the phenomenon over a period of time. The timeframe for this study was cross-sectional as the compliance behaviour of employees was studied at a point in time

(Saunders et al., 2012). A cross-sectional timeframe was also best suited, given the time and resource constraints associated with this research.

4.5 Data Collection Instrument

Semi-structured interviews will be the primary source of data for this study, which is consistent with the research strategy adopted. Semi-structured interviews also afford the researcher the flexibility to adapt to different interviewees (Noor, 2008; Mohajan, 2018), while the interview guide ensures consistency in thematic approach (Qu & Dumay, 2011). In addition, because data collection and analysis overlaps in case studies and interviews, it allows the researcher to modify questions during the research and potentially improve the relevance of the research instrument (Bhattacharjee, 2012). This overlapping also enables the researcher to reorientate the theoretical framework, allowing the theoretical work, the empirical work, and the case to evolve simultaneously (Dubois & Gadde, 2002).

Secondary data was gathered from ISP documentation, official company communication on espoused culture, and reports to supplement primary interview data. Some secondary data however was only accessible from within the organisation's network, such as documents from its intranet website. The secondary data facilitated data triangulation, which is recommended to corroborate evidence, and strengthen findings (Rowley, 2002; Kaplan & Maxwell, 2005; Yin, 2009). For example, a phishing simulation report was used to corroborate primary interview data to establish the level of employee compliance behaviour, which answered this study's secondary research question. All data types collected from primary and secondary data sources were qualitative in nature.

Interview Guide

The semi-structured interview questions were developed in accordance with the concepts outlined in the theoretical framework. The semi-structured interview questions were informed by the research question, extant literature, and the theoretical framework, as is recommended (Rowley, 2012). The nature of the guiding questions were open-ended to encourage participants to share their own experiences and to facilitate discovery (Roberts, 2020). The questions, outlined in Appendix A, were intended to serve as an interview guide. The open-ended questions were intended to guide the examination of information security culture, social structures, cultural orientations, and cultural contradictions that emerged. The

interviews were recorded and transcribed before the next interview was conducted, as is recommended (Saunders, et al., 2012). All data pertaining to the research were stored in the NVivo software package.

4.6 Data Collected

All interview data were collected using the interview guide's semi-structured questions. All interviews were conducted virtually via Microsoft Teams. The interviews lasted 45 minutes on average, of which the first 5 minutes of each interview was reserved for introductions and contextualising the research. The interviewer also utilised this time to reiterate the ethical considerations of the study and reassure participants of their confidentiality and anonymity. To that end, all the names of the participants were replaced with pseudonyms, to preserve anonymity and to mitigate any associations with the data during analysis, as all interviews were conducted by the researcher.

A total of 18 participants were interviewed across varying job roles and departments, as depicted in Table 2. Most of the interviews, 15 in total, were conducted with video enabled. The researcher transcribed the first 9 interviews, while an external transcriber completed the last 9.

Table 2. Interview Participants

Name	Department	Years of Service	Occupation	Team
IPT1	Information Systems	7 and above	Security Specialist	Security
IPT2	Logistics & Distribution	7 and above	Delivery Claims Investigator	Service Operations
IPT3	Information Systems	7 and above	Systems Analyst	Application Development
IPT4	Information Systems	5-7	Solution Specialist	Health Safety Environmental and Quality (HSEQ) and Legal
IPT5	Information Systems	5-7	Solution Specialist	HSEQ and Legal

IPT6	Information Systems	7 and above	Technical Analyst	Technical Support
IPT7	Retail	7 and above	SAP Real Estate Master Data Specialist	Retail Assets
IPT8	Information Systems	3-5	End User Support	End User Support
IPT9	Information Systems	7 and above	Principal Solution Design Specialist	Application Development
IPT10	Information Systems	7 and above	Senior SAP Basis Specialist	SAP Basis
IPT11	Information Systems	1-3	Service Desk Specialist	Service Operations
IPT12	IT Audit	7 and above	Advanced Analytics & Assurance Specialist	Enterprise Risk & Assurance
IPT13	Information Systems	7 and above	Technical Analyst	Technical Support
IPT14	Information Systems	7 and above	IT Manager: Infrastructure and Operations	Infrastructure and Operations
IPT15	Information Systems	0-1	Security Specialist	Security
IPT16	Information Systems	7 and above	Integration Architect	Architecture
IPT17	Information Systems	7 and above	IT Manager: Applications and Support	Application Development
IPT18	Information Systems	7 and above	Chief Information Officer	Chief Information Officer

4.7 Data Analysis

This research followed an abductive approach to data analysis, where the researcher infers theoretical patterns from the collected data and locates the identified themes in a conceptual

framework (Saunders et al., 2012). The qualitative data was analysed using thematic analysis, used for identifying emerging patterns within the data (Braun & Clarke, 2006).

Analysis in qualitative research is generally dependent on some form of interpretation and explanations of meaning (Alhojailan, 2012). Qualitative analysis, according to Namey et al. (2008), is generally categorised as either content or thematic in its analysis. Content analysis is a systematic approach to coding and categorising large amounts of textual data by using the frequency of keywords, synonyms, their relationships, and structures (Vaismoradi, Turunen, & Bondas, 2013). This unobtrusive technique requires minimal interpretation and is therefore valued for its efficiency and reliability. A primary drawback of content analysis is the possibility of contextual constraint due to the significance associated with word frequency, thereby limiting richness in data and in the final report.

Thematic analysis on the other hand is more nuanced and involved, emphasising context (Vaismoradi, et al., 2013). The technique involves the systematic identification and organisation of patterns of meanings, offering insights into themes within data (Braun & Clarke, 2006). Thematic analysis is intended to go beyond word frequency and descriptive analysis by focusing on semantic and latent meanings within the data (Namey, et al., 2008). Braun and Clarke (2012) point out that the strength of thematic analysis is found in its accessibility and flexibility of approach. It is accessible in that it can provide a novice researcher with a method for analysing qualitative data systematically. It is flexible in that it is only a method as opposed to an approach, which makes it compatible with both inductive and deductive approaches to research. However, coding and analysis is generally a combination of both approaches (Braun & Clarke, 2012), which makes it appropriate for this research which follows an abductive approach to analysis. Furthermore, thematic analysis is most appropriate when the research question requires the identification of influencing factors (Alhojailan, 2012), such as a participant's interpretations which could explain their information security compliance behaviour. Thematic analysis was therefore selected as an appropriate method of analysis for this research.

Thematic analysis commonly involves the initial coding of themes followed by sub-themes. The NVivo software package was used as a data store and as the primary data analysis tool. This research adopted Braun and Clarke's (2012) recommended six-phased approach to thematic analysis, which was the framework used to conduct thematic analysis in this study, as shown in Table 3.

Table 3. Six phases of Thematic Analysis (Braun & Clarke, 2006)

Phase	Activity	Description
1	Familiarise yourself with the data.	Read and re-read data, making notes of initial ideas. The researcher read all the transcripts during this phase, including transcriptions from the external transcriber.
2	Generating initial codes.	Generate semantic or latent labels that identify features of the data and meanings that are potentially relevant to the research question. During this phase the researcher accumulated 183 codes that were initially deemed relevant to the research question.
3	Searching for themes.	Analysis progresses from codes to themes, which captures important patterns or meanings relevant to the research question within the data. Searching for themes is an active process of theme generation. During this phase the researcher used initial codes to search for recurring patterns that could be regarded as themes and sub-themes.
4	Reviewing potential themes.	A recursive process of reviewing themes in relation to codes and the entire dataset and its relevance in answering the research question. The themes and sub-themes were reviewed during this phase to ensure distinction and relevance. Some themes were merged while others were discarded.
5	Defining and naming themes.	Develop an analytical narrative clearly stating the uniqueness and relevance of each theme in relation to the research question. Each theme was analysed in detail in relation to the larger research question, and changed to more informative names.
6	Producing the report.	Producing a report and a final analysis with a selection of compelling data extracts, relating them to the research question. During this phase the researcher synthesised the themes to produce a report of the analytical narrative.

4.8 Ethical Considerations and Confidentially

Ethical considerations are essential as they protect the interests of participants and inhibit the researcher from manipulating results (Bhattacharjee, 2012). Access authorisation was obtained from the management of the selected organisation. All participants were informed of their voluntary participation. Their identity remained confidential and anonymous, and they could exit the study at any stage. Ethical approval was also obtained from the University of Cape Town Ethics Committee.

4.9 Summary

Following is a summary of the methodological approach used to answer the research questions at hand. The research philosophy and approach underpinning the choice of research design, the adopted research design, the choice of research methods, the data collection and analysis techniques are summarised in Table 4.

Table 4. Research Methodology Summary

Dimension	Choice	Justification
Ontology	Subjectivist	A subjectivist ontology is more consistent with the proposed theoretical framework, which is grounded in Structuration Theory (Giddens, 1984).
Epistemology	Interpretivist	Closely aligned to the structural framing around Structuration Theory (Giddens, 1984).
Approach	Abductive	This study continuously moved between the theoretical framework and empirical data, which is consistent with abductive reasoning (Dubois & Gadde, 2002).
Research Strategy	Single case study	A single case study was most feasible given the time and resource constraints of this study (Eisenhardt, 1989). The case was appropriate as it represented an organisation with Information Security policies and diverse cultures. The subcultures achieved variance

		along the dimensions of the theoretical framework (Seawright & Gerring, 2008).
Timeframe	Cross-sectional	A cross-sectional timeframe was best suited, given the time and resource constraints associated with this study (Saunders, et al., 2012).
Data Collection - Sampling	Purposive Sampling	Participants were selected from various departments and roles representing multiple subcultures.
Data Collection - Procedure	Semi-structured interviews	Semi-structured interviews were consistent with the adopted research strategy. It also afforded flexibility to adapt the interview guide and reorientate the theoretical framework, while ensuring consistency in the thematic approach (Dubois & Gadde, 2002; Qu & Dumay, 2011; Mohajan, 2018).
Data Analysis	Thematic Analysis	Thematic analysis is compatible with both inductive and deductive approaches, which makes it appropriate for abductive studies (Braun & Clarke, 2012). It was also the most accessible method to the researcher for analysing qualitative data. Furthermore, thematic analysis is most appropriate when the research question involves the identification of influencing factors, as is this study necessitates (Alhojailan, 2012).

5 Analysis and Findings

5.1 Case Description

The selected case was a large South African organisation which was majority-owned by a Southeast Asian organisation. Pseudonyms were used for the organisations so as to maintain the confidentiality and anonymity of the case and its participants. The subsidiary organisation in South Africa was subsequently renamed to ORG₁, while the Southeast Asian parent organisation was renamed to ORG₂. This study also adopted a similar approach to Yayla and Lei (2018) in conceptualising culture in a multinational organisation. The subsidiary organisational culture was regarded as separate and distinct from the parent organisation.

The organisation had established ISPs and a security awareness programme, which included phishing simulations to evaluate the level of compliance behaviour among employees. The organisation's security awareness programme existed in the form of online training lessons, which the organisation termed "Cyber Security Training", where participation was compulsory for all employees. Furthermore, the information security training lessons were complemented by associated phishing simulations as part of the same awareness programme. The phishing simulation entailed sending deceptive emails to employees, and thereby simulating malicious intent, and gauging the organisation's potential response to legitimate phishing attacks. The phishing simulations was an information security initiative and was conducted exclusively by the organisation's information security team. The following section discusses the role of the organisation's cyber security training programme, and the level of compliance behaviour among employees.

5.2 Information Security Compliance Behaviour

The following section describes the identified level of compliance behaviour as reflected by the gathered data, with the aim of answering the secondary research question of this study. There appeared to be a reasonable degree of awareness of information security risk among employees. This was in large part due to the information security awareness program that the organisation implemented.

5.2.1 Information Security Training

All 18 participants referred to the organisation's information security training program during the interviews. Most of the research participants indicated that the company's Cyber Security training program has indeed increased their level of security awareness. For example, a claims investigator reflected on how his compliance behaviour changed after doing the training:

Now because of our cyber security lessons that we've learned... I came to realise that I'm sharing a lot of information with him, that might not be that necessary. And hence with that courses that we've done, I started to change the way I'm doing it, yeah.

Likewise, a solution architect expressed the same perception:

I do believe that after everyone has gone through this training awareness program, almost all of the employees have a much better understanding of what Information Technology (IT) security entails and the seriousness and repercussions of it, and not being compliant.

An IT manager made similar comments about the effects of the information security training program on security awareness "But I think we're getting there where people are getting a lot better at it". This is further substantiated by an analysis of secondary data, which shows the positive impact of the organisation's Cyber Security Training on the information security compliance behaviour of employees. In 2021 the organisation conducted four Cyber Security Training campaigns accompanied by phishing simulations, as shown in Table 5. There was a three-month interval between Campaign 1 and Campaign 2, three months between Campaign 2 and Campaign 3, and a one-month interval between Campaign 3 and Campaign 4. The resulting trend shows that as the training increased, the subsequent failed phishing simulations decreased.

Table 5. Security Awareness Simulations

Campaign 1 May 2021	Campaign 2 August 2021	Campaign 3 October 2021	Campaign 4 November 2021
7% - failed	36.8% - failed	4.6% - failed	0.6% - failed

Furthermore, the information security training program applied to all employees, including top management. As a solution specialist stated “It was compulsory for everyone. It was compulsory from the CEO to the guy that delivers our mail from the mailing department”. The visible participation of top management in information security initiatives of this kind is important for the cultivation of an information security compliant culture, as it shows that the organisation’s top management is serious about the content communicated in the information security awareness training.

5.2.2 The Information Security Compliance Behaviour Level

While the above sentiments were broadly reiterated by participants, there was a strong indication that although the Cyber Security Training program is effective, it is still insufficient. An IT manager for example stated:

And we’re great at driving phishing and cyber security risk of people stealing your information and identities and getting access to information so we’ve been great in that in the past year or two but haven’t been great in terms of creating awareness around information and management of information, you know there’s still people printing a lot of stuff off and just leaving it all over the show in hard copy format information and people have access to it, contracts, vending information.

A security specialist and the Chief Information Officer (CIO) confirmed the same:

They get to do all these things, and then I guarantee you, and that is based on what we can see when we do cyber security campaigns. It’s actually quite amazing, but you send a link to somebody, and this thing looks exactly like the log in screen, like for instance their email. And you would think people that work in IT would spot the difference.

So, compliance as part of the culture, will be driven by expectations that are set by Human Resources (HR) for the way employees should be behaving. And does ORG1 have a compliance culture? On a scale of one to ten, probably about a six to seven.

The information security awareness program has certainly been effective in raising awareness, but it appeared to fall short of instilling a desired degree of compliance behaviour among employees and creating a security culture. This was widely agreed upon by

participants who observed that non-compliant behaviour from employees and management alike was common within the organisation. For example, a systems analyst, a technical analyst, and a principal solution design specialist commented on the level of information security compliance behaviour “But then coming back to information security. I think that most, if not all of us, are guilty of that”, “Yeah, I've seen lots of stuff with people share passwords”, and “I don’t think our colleagues, or our employees, or now I’m just speaking generally, generally are always, always have that security mindset, man”. This was corroborated by an analysis of secondary data obtained from the phishing simulation results, as displayed in Table 6. Phishing simulation emails were sent to approximately 3400 employees. While the failure rate appeared to decrease, there were still 1834 first time failures in total and an alarming rate of repeat failures. Although the statistics give a simplistic view of the compliance behaviour rate, as it includes phishing attacks only, it does however provide some validation of primary interview data.

Table 6. Phishing Simulation Report

Failed Simulation x 1	Failed Simulation x 2	Failed Simulation x 3	Failed Simulation x 3+
1834	527	98	15

Employees who fail a phishing exercise were obligated to attend additional information security training. As depicted in Table 6, the report shows that 1834 users failed the phishing simulation once, 527 users failed twice, 98 users failed thrice, and 15 users clicked more than three times. Thus, in answering the secondary research question by establishing the level of compliance behaviour, the general level of compliance behaviour among employees was uninspiring and average at best. Having addressed the secondary research question by establishing the level of compliance behaviour, following is an analysis of the cultural orientations within the case.

5.3 Analysis of Culture

The organisation’s culture was interrogated for varying cultural orientations in accordance with the CVF (Cameron & Quinn, 2011). The four cultural orientations of the CVF are rule orientation, goal orientation, support orientation and innovation orientation. (Faerman & Quinn, 1985; Cameron & Quinn, 2011). Rule orientation, or hierarchy cultures, have a strong

focus on internal processes and structures that facilitate stability and control. Goal orientation, or market cultures, are externally focused and maintain a degree of control by setting goals for employees to achieve (Quinn et al., 1991). Support orientation, or clan cultures, are internally focused and emphasise flexibility in their structures (Faerman & Quinn, 1985). Innovation orientation, or adhocracy cultures, are externally focussed with a strong emphasis on flexibility (Quinn & Rohrbaugh, 1983).

5.3.1 Rule Orientation

Cultural variances are apparent in the examined groups for support, goal and innovation orientations. An examination of rule orientation however revealed less cultural variance and more uniformity between teams. All participants believed the organisation had established rules and procedures in place, while still affording employees a reasonable degree of autonomy. For example, a real estate master data specialist in the retail department stated “I have the freedom to do my work the way I want to, however it has to be done, and within the system”. Similarly, a principal solution design specialist expressed the same sentiments “The performance is just evaluated on what needs to be done. We are not evaluated on how it needs to be run”. The notion of rules and procedures with autonomy extended to tasks to be performed. The measure of rules and procedures which govern tasks varied based on the nature of the task at hand. For example, any task that required engagement with, what the organisation deems, a core and critical information system, invoked stricter governance rules. To illustrate, a systems analyst explained the governance principles applied to the core Systems Analysis Program Development (SAP) system “So that is governed by procedure and how those applications connect into S4, and stuff like that. But when it comes to managing the actual developers and managing their work, you can take various approaches to do that”.

Likewise, an excerpt of a solution specialist’s answer during the interview:

Yes, I'm free to do what I want in a certain space, and how I want to do it in a certain space. But I also need to be in the boundary, in boundaries. I can do research and get a solution which are off the shelf, or we can custom build a solution... But whichever solution you aspire to look at. We do have a governing body... They called the Architecture Quality and Assurance group, and they usually provide us governance requirements and implementation when we implement a solution.

The same variance in strictness of rules and procedures, based on the nature of the task at hand, was the same for all teams. The organisation therefore had a fairly uniform orientation towards rules and procedures. However, the reasonable measure of autonomy afforded to employees leads to an inference that rule orientation is not the salient culture type. According to Cameron and Quinn (2011), rules and procedures which govern all that people do is a key characteristic of rule orientated cultures. Furthermore, stability and predictability are the primary criteria for effectiveness (Faerman & Quinn, 1985).

5.3.2 Goal Orientation

Goal-setting appeared to be embedded in the organisation's performance evaluation process, which is a characteristic of goal orientated cultures (Quinn et al., 1991). Most participants expressed that their goals are set by management, while some indicated that goal-setting exercises were a collaborative effort between individuals and management. For example, a senior SAP basis specialist stated, "the performance is based on just what they give you and not anything else". While a delivery claims investigator indicated "So, I think it's a collective effect, when we talk about, you know, determining what is the targets, what is the goals for that particular year. So far that has been my experience". Regardless of whether goal-setting was a coordinated or uncoordinated effort, participants generally believed that their goals aligned with the organisation's overall strategic vision. For example, a systems analyst commented "So ultimately the goals is set on more a strategic type of view. Where it, sort of, trickles down from a high level strategic position to a tactical, and then to operations". This is in keeping with good goal-setting practices, as goals should ideally be aligned with the organisation's mission at large, and should be attainable and time-bound (Cameron & Quinn, 2011).

Furthermore, goals are also a means of holding employees accountable for their reported actions and rewarding accomplishments (Van Muijen, et al., 1999). As a systems analyst in the development team stated, "And the good thing about goals, I suppose, it means that you have your own responsibilities...but as I suppose when it when it comes to setting goals, you are ultimately accountable for reaching their goals". When asked whether their individual goals aligned with the organisation's information security goals, a senior technical specialist however stated, "Absolutely...I can definitely see how important those three aspects are. And there are controls in place for each and every measure that I've mentioned now. And I see it

now, I see it now”. Thus, of all the participants, only one believed that their individual goals aligned with the information security goals of the organisation.

In addition, secondary data was analysed in the form of official communication from the HR department, which indicated its stance on cultural values. The organisation views accountability as a cultural value needed for employees to achieve their goals. According to Van Muijen et al. (1999), contingent rewards and accountability characterise goal orientated cultures. As extracts from internal communication published on the organisation’s intranet platform in 2020 revealed:

We know the Culture of Accountability is the most effective culture within an organisation where employees make a personal choice to rise above their circumstances and demonstrate the ownership necessary to achieve key results. This year, our focus will be on strengthening the Culture of Accountability.

The organisation also used culture management tools to help employees accelerate cultural changes. For example, the organisation encouraged employees to publicly acknowledge colleagues who demonstrate the organisation’s core cultural beliefs of loyalty, integrity, professionalism, and cohesiveness. The organisation believed professionalism can be achieved by taking ownership and striving for excellence, which is consistent with goal orientated cultures that favour commitment to excellence and achieving exceptional results. As an internal newsletter on cultural values stated, “Since the introduction of the Cultural Beliefs in 2015/6 (Results Matter-Own It-Focused Execution-Nurture Trust-Tell Me-Shared Success), we have witnessed many key change milestones in the ORG₂ ecosystem... These Cultural Beliefs are our shared values in motion”. These values were consistent with stipulations on the organisation’s external internet page:

The values we strive to embody are: Loyalty (to corporation), Integrity (honest and upright), Professionalism (strive for excellence) and Cohesiveness (united, trust and respect for each other). The goal of adding value in a balanced manner is our driving force.

Goal orientation therefore appeared to be integral to the organisation’s performance evaluation process and overall espoused culture. It was therefore safe to assume that the organisation indeed had a reasonably goal-orientated culture. Although the goal-setting

process appeared to vary from team to team, all performances were evaluated on goal achievements, which was consistent with the organisation's espoused value of professionalism.

5.3.3 Support Orientation

The degree of support orientation varied among the different teams. Most participants confirmed a measure of mutual support and trust within their teams. However, the level of trust and support experienced within the various teams seldom exceeded professional trust within the workplace. For example, an advanced analytics and assurance specialist in auditing observed "I mean, we trust on a professional level, access to systems, how to build the system, but I do not think we are up to that level where we trust". Likewise, a senior technical specialist experienced comparable levels of support with their team:

There isn't much interaction on a personal. It's all mostly work related. And if you do chat about work, I do think we do personal chat as well. But that's about the only time that we chat to each other.

While there appeared to be a strong measure of support within teams, trust rarely extended beyond the workplace and into their personal lives. This evidence suggests that the organisation had a strong orientation towards professional cultures, although to varying degrees per team. For example, a security specialist indicated a high level of professional trust was needed among team members, given the sensitive nature of some of their tasks:

So, there is a level of trust, and only where your work is concerned, obviously. That you can trust somebody with sensitive information. Like for instance, if there's an incident, we need to come together as a team to do incidence response and all that kind of stuff...So it comes with the role.

It was also clear that the extent of mutual support varied within the same team, which seems to suggest the existence of subcultures. One systems analyst observed "Our team is very big. There are certain people in the team that share trust or have trust in more in one another than others. But I think it's more on the team that closely work together". Likewise, a SAP real estate master data specialist within the retail department indicated similar varying levels of trust "I think Glenda and Melanie would probably have more to do with each other because they work with maintenance...My work, because of the nature of it...I work closely with

Ben”. The organisation in general had a broadly professional culture, with a strong measure of trust within the workplace. This was corroborated by an IT manager’s explanation of the organisation’s cultural aspirations:

There is a change that we are trying to drive in the culture, which is a ORG₂ thing as well. And it is really more of a team culture of being professional. And being professional and having integrity and ethics and things like that.

5.3.4 Innovation Orientation

There was evidence that the cultural orientation of innovation varied between teams, and even within the same team. For example, a systems analyst within the development team stated:

So I think that innovation is big within the team. But I think only in certain teams and not all teams. So if you were to speak to a service desk consultant, or service desk agent, whatever, he’ll tell you a completely different story about how they drive innovation within the team. So the dynamic changes across teams.

While a principal solution design specialist within the same team said about innovative initiatives “Now at the moment, no. Our focus now is just to work a bit more effectively as a team”. Regardless of how participants experienced the degree of emphasis on innovation, there appeared to be a common drive within the organisation in general to “work a bit more effectively” and improve current processes. This was corroborated when analysing secondary data in the form of company newsletters and intranet documentation. The organisation embarked on a journey to continuously improve daily processes in a collaborative manner, which the organisation termed “New Ways of Working”. For example, an extract of an intranet webpage posted in 2017 showed the company’s inaugural efforts to facilitate this process:

Following the opening of the New Ways of Working gallery at the Head Office on Thursday 9th November.... The spaces are designed to enable colleagues to learn about the New Ways of Working in a relaxed and engaging environment as well as offering the chance to connect and discuss ideas.

Likewise, an advanced analytics and assurance specialist within the auditing department reflected the same, saying “they actually encourage people to come up with new ideas, doing things differently, doing things better”. Some participants indicated that they were expected to improve existing processes by means of automation. A security specialist for example stated:

I think a big focus is on automation. To kind of get rid of all the mundane tasks and stuff that you’re busy with every day. So there's always a drive or to get new technology in, to enforce controls, but in a better way. So I think to free up security people to do more research and come up with better ways of working.

Although encouraged by the organisation, it appeared as though innovation was not explicitly rewarded within teams. There is no clear indication that individual performances were evaluated based on innovation, although it was encouraged. When asked if innovation was included in their performance goals, a systems analyst stated, “Not from that perspective no. But it is encouraged in the team though”. However, in analysing secondary data on the organisation’s intranet platform, it was evident that innovation was in fact a key cultural value. As public acknowledgements on an intranet newsletter stated:

Here’s what INNOVATE NOW looks like to me: I challenge norms and push boundaries. David’s continued commitment and relentless efforts have accelerated progress to fostering the transition to a more data-driven organisation, a key enabler to deliver on our ambitions.

This implied that innovation, although not explicitly evaluated in performance contracts, was indeed encouraged and was an intentional cultural posture held by the organisation.

5.3.5 Information Security Culture

Information security culture is generally defined as the values, attitudes and assumptions about information security which are shared by members of an organisation (Da Veiga & Eloff, 2010). Information security knowledge and awareness is a key dimension of an information security culture (Nasir, et al., 2019). Analysis of results suggested that, although cyber security awareness was high, information security awareness however was relatively low. Most participants perceived a lack of information security knowledge and awareness among colleagues, which is corroborated by the low level of compliance. As an advanced

analytics and assurance specialist stated, “I think, it is one thing to reprimand, but you would find that most of the time a lot of the guys, I do not want to say ignorance, but they did not know”. Similarly, a security specialist explained “But I think the security team, they need to make sure people understand their responsibility because a lot of people genuinely, do not know”.

The level of awareness among employees gives some indication of the organisation’s security culture maturity level. Top management support for information security is another dimension reflective of information security culture (Solomon & Brown, 2021). Results showed that information security management and information asset management, in the form of data classification, were respectively regarded as immature and in its infant stages. For example, an IT manager explained:

I think there’s insufficient classification and we’re relying on individuals to have a better understanding...so we've left it a lot up to the individual to say what information is critical...So I think ORG₁ has been very slow off the block and we've been talking about it probably for about 5/6/7 years in terms of classification of information... we’ve got a lot of good systems and technology in place, I don’t think we are as mature as what we think we are.

Furthermore, in commenting on the organisation’s progression in cultivating an information security culture, a security specialist stated, “Now, it will come over time...where we are now within ORG₁, ten years from now the culture that you are describing, will be here because remember the governance framework is not even a year old yet”. Similarly, the CIO, commenting on the present state of the organisation’s information security culture, stated:

I think the important thing here, you have to cascade culture from the top. In other words, at organisational level and then as it cascades down into security behaviour. You will not be able to set a specific security culture if the overall higher-level culture in the organisation is of non-compliance.

Thus, although the foundations were being placed, it can be safely deduced that the organisation’s information security culture was in a state of immaturity. Following is an analysis of cultural contradictions and conflict, and their effect on information security compliance behaviour.

5.4 Cultural Contradictions

Cultural contradictions, according to Walsham (2002), arise from differences of interest between groups, such as divergent goals, priorities, values, or professional affiliations. Contradictions also form the basis for potential conflict that could arise, which has negative implications on information security compliance behaviour (Karlsson et al., 2018).

The aspect of contradictions was explicitly examined using Geeling et al.'s (2020) illustration of the five types of cultural contradictions that could emerge as a result of cultural differences. There was strong evidence of four types of contradictions, namely Priority Contradictions, Process Contradictions, Vision Contradictions, and Technology Contradictions. There was little evidence of Role Contradictions among participants. There seems to be a good understanding of the respective roles and responsibilities of individuals and the security team as it relates to information security compliance behaviour. Most participants indicated that information security is everyone's responsibility. As an advanced analytics and assurance specialist in the auditing team stated, "I think, it is everyone. That component should be ingrained in your culture. We should not make it the responsibility of one team, because then you are going to create a them and an us". A technical analyst in the infrastructure and operations team expressed the same understanding of roles:

I would say we all have a role to play because it comes out to be behaviour as well, especially with the phishing exercises and stuff like that, to know what you're looking for. So I would say you also need to educate yourself.

While Role Contradictions did not emerge as a factor in analysis, the remaining four forms of contradictions did, which are discussed in the following sub-sections.

5.4.1 Priority Contradictions

Priority Contradictions occur as a result of differences in values systems which inform the prioritisation of tasks, in this study information security compliance behaviour (Geeling, et al., 2020). Only one participant, a solution specialist, expressed no contradictions in priorities when comparing ISPs with his own responsibilities on a project, "Any breach can lead to great financial or reputational damage. And besides the financial damage, reputational damages are even worse sometimes. So I would say high priority". All other participants expressed perceived differences in priorities between their professional duties and

information security measures. The researcher's observations of visible and audible queues presented during interviews revealed immoderate levels of frustration and agitation from participants when asked about priorities. As a delivery claims investigator explains:

I haven't heard of much security breaches happening within ORG₁, since I've been working here... So I was under the impression, given the fact that this is now not the case, why would our security be placed at that high level, in terms of a priority?

Although there appeared to be an acceptance that information security is necessary and should be a high priority, employees were clearly questioning the criticality of information security when compared to their own goals and tasks of supporting the business. As a SAP real estate master data specialist said:

I understand the need for security...Because we can have every security system in the world up and running. It can be major first world...But if you don't have an organisation to apply it to because your rules are stopping you from actually doing business.

It is also clear that contradictions in priorities can indeed lead to conflict, which according to Giddens (1984), is the actual behaviour that ensues as a result of divergent interest. Of interest to this study is contradictions which breed conflict, expressed as information security non-compliant behaviour. Evidence of this expression of conflict was found as the same participant further explained:

I think, there are times when I ignore security policies because I need to get something done, so I actually don't care. And I know that's wrong. I shouldn't say I don't care, I do care, but I understand the foolhardiness of what they're wanting, compared to what I actually need now.

This was reiterated by an IT manager:

There're a lot of people who don't comply, but not intentionally. And all they're doing is they're wanting to get things done, so that's why they don't comply, because they're not any the wiser and all they're thinking is I'm doing my job.

A principal solution design specialist suggested the need for a compromise between information security and non-security personnel:

Bring that in their conversation and let them rather discuss it, you know, get talking then rather forcing, you know, and let us come to a compromise for you to get what you want and for security to get what we want.

It was apparent that Priority Contradictions were indeed common, leading to feelings of frustration on the part of individuals, and a perception that information security hinders and impacts their performance. This essentially created a negative perception about information security and security personnel in general.

5.4.2 Process Contradictions

Process contradictions can emerge if there are differences in work practices arising from divergent values and assumptions between groups and individuals (Geeling, et al., 2020). Differences in work practices usually require a change in processes and procedures. This change in processes can become cumbersome for employees. The data revealed strong evidence of Process Contradictions. A solution specialist in the solution design area expressed no Process Contradictions, which was consistent with the explanations given to Priority Contradictions. The same participant did however voice a moderate level of frustration, “Absolutely. It’s like a thorn in your side. But, it needs to be done. It’s one of those things that needs to be done. Otherwise, you’re not compliant”. This could indicate that those who have found no Process Contradictions, have in fact compromised and taken action to address potential conflict, by either adapting their own processes to accommodate information security, or by developing their own workarounds to subvert policies (Davison & Ou, 2018). Walsham (2002) found similar instances of team members learning over time to compromise, to the overall benefit of the organisation, in much the same way as Geeling et al. (2017) found a coordinated culture to be produced where an accommodation is reached.

In this case study however, it seemed the salient culture value as it pertains to processes is indeed in contradiction with information security values. There was not enough systemness of a coordinated culture displayed within the data for it to be regarded as shared by members. Hence, most participants expressed contradictions and conflict between their daily practices and information security processes. For example, a senior SAP basis specialist explained how information security processes conflicted with his daily task:

So now it happens a lot where you try to complete a job, but you do not have the necessary access. But the policy says but you are not supposed to have that and then I clash with that all the time.

Likewise, a technical specialist explained how a new information security process forced a change in his daily practices, which in turn impacts his efficiency:

Yeah, especially that Privileged Access Management (PIM) thing that they implemented...I understand where they're coming from, but it makes your daily work difficult. Because you used to doing it a certain way, and you fluent in your way...Almost like you must now jump over three guys to get to the door... Because it's now taking you longer to do something that would've taken you 5 seconds. Now it's taking you a couple of minutes to complete.

The data also revealed that, similar to an analysis of Priority Contradictions, the terms frustration and hindrance were often used in answering process contradiction questions. As an end user support engineer stated, "Yeah, like that gets more frustrating sometimes, especially when you, you need to get something out, let's say now you got this project that needs to be done". It was therefore evident that Process Contradictions, leading to feelings of frustration, and being perceived as impacting an individual's ability to efficiently perform daily tasks, was a theme that emerged from the data.

5.4.3 Technology Contradictions

Technology contradictions are likely to arise from differences in assumptions and beliefs about technology and its embedded functionality (Geeling, et al., 2020). The extent to which an information system, and its embedded functionality, appropriately fit the expectations and experiences of employees, can give rise to these differences. Groups are more likely to accept and adopt information security technology, if the values embedded in the technology and policies adequately match the values of individuals (Leidner & Kayworth, 2006). In this study, the degree of acceptance of information security was therefore associated with the degree of fit between information security systems, with their embedded policies, and the individuals engaging with it.

Consistent with an analysis of Priority and Process Contradictions, there were strong suggestions of Technology Contradictions within the data. Of all the participants, a SAP real

estate master data specialist was the only participant who experienced no contradictions in technology. There appeared to be an understanding that information security technology, with its embedded policies, are there for the protection of individuals and the organisation. This understanding appeared to have a bearing on information security acceptance and the willingness to compromise. As the participant expressed “So I would be lying if I said it did. I’d like to say so, but it didn’t...In fact, it’s been to our benefit”. However, the same participant’s experience of embedded security policies within technology was not shared by participants. There was an overwhelming sense of Technology Contradictions among participants. For example, a delivery claims investigator explained how a Virtual Private Network (VPN) solution that was implemented impacted his ability to download content from the intranet and internet “And I believe VPN is like a security measure as well to protect you. And yet it’s just somehow a bit slower when you want to download. So that could maybe take a bit longer to get things done”. This sentiment was echoed by a service desk specialist, who bemoaned the same experiences with the organisation’s VPN and implementation:

We have this now, antivirus. It is working fine now. But in the beginning...Actually, even now there are people that are still struggling with it a lot...So, I have experienced that, and at times it just did not work well. And also, actually even VPN...at times it will be very slow.

Participants further expressed a sense of frustration, as an information security browsing policy and technology stopped them from accessing certain content which could be pertinent to their job roles. This was illustrated by a systems analyst who stated:

But it can also be a bit of a deterrent for the organisation, because you're not allowed the flexibility to perform your task as you would need because you are governed by that policy, and certain of the of resources are blocked by the organisation. And that could be resources that could be very valuable for sustaining the organisation and also for the future of the organisation from a value point of view, and also from a profit point of view.

Similarly, a solution specialist explained:

They also blocked the YouTube website and other social media websites that was blocked. And me doing research constantly on new solutions, it does have a slight impact when doing some research on particular solutions using that, if I may be used, because in that case I will have to use my mobile phone.

It was clear from analysis that there was strong evidence for Technology Contradictions among teams. It was also apparent that participants largely agreed that information security technology was required and should be prioritised. However, individuals appeared to regret the impact it had on their ability to perform their daily tasks with efficiency. As an advanced analytics and assurance specialist elaborated on his team's experience with a new Identity Management System that was implemented:

the guys actually doing the work, they felt that they were being hampered in actually effectively doing their work, where the guys from security think, "No, but we are only ticking a box. We are only securing. This is what we are doing." But before you implement anything, just go back and review what you have done is actually a working solution.

While still maintaining that information security should take the highest priority "I think, actually needs to be the highest priority... Any breach or whatever could cause the downfall of your company, potentially or reputational and financial harm". The analysis also showed similar results to Priority and Process Contradictions, where the terms hindrance, frustration and impede were often used in answering Technology Contradiction related questions. This indicated that contradictions, in the form of priorities, processes and technology, lead to feelings of frustration, and have a perceived impact on an individual's performance and productivity. This can lead to a negative perception of information security and information security personnel in general, which was an unexpected theme that emerged. The negative perceptions of information security as impacting individual performance was examined as an emerging theme with Structuration Theory as the analytical lens.

5.4.4 Vision Contradictions

Vision Contradictions can arise as a result of misaligned goals between stakeholders who are engaging with information systems development (Geeling, et al., 2020) – applicable in this study to information security. The alignment of organisational goals and information security goals is essential for good information security management (Ramachandran et al., 2013).

There was an alignment between the organisation's overall goal, and the implementation of information security measures. For example, both information security personnel and management understood an alignment between the organisation's overall goals and that of information security. As an IT manager stated when asked about the organisation's information security goals:

So yes, we do, and it's based on how they've rated the risk. So, there's an information security policy and there's the risk, cyber security risk and information security risk...And based on that we've set ourselves a goal for the next 3 years of what we need to implement and change to improve that. So, there're definitely goals in place, and part of that is all these programmes you've seen come through.

Likewise, a security specialist answered:

The company is only now recognizing cyber security or information security. And why I'm saying that is because it is part of the kind of company KPI is or something like that. And it's measured on that as well. So, it's only now that it's getting visibility, and I think it's getting this visibility because of all the ransomware attacks and all that kind of stuff. And it is being brought to management attention, in a little bit higher.

These findings suggested that goals were aligned between the organisation and information security, as per the understanding of management and security personnel. There was however a lesser understanding of those information security goals held by the organisation when analysing data from non-security personnel. Most non-security participants were unaware or unsure of any information security goals espoused by the organisation. For example, a senior SAP basis specialist explained that members of the SAP team had no knowledge of information security goals: "I have not heard of anything. I think, to tell you the truth, I do not think it is being preached enough about information security. So that is what it is".

Likewise, a delivery within the logistics and distribution department had the same experience: "I don't think I've been...privy to a discussion with my manager, as an example, on an item of a security measures within our particular performance contract". A principal solution design specialist stated, "No. Not that I know of".

The misalignment of information security goals was therefore an emerging theme in analysis. The effects of this misalignment was examined further in a subsequent section with the use of Structuration Theory as the analytical lens.

5.4.5 Conflict and Non-Compliant Behaviour

Contradictions, defined as divergent values, norms and practices held by individuals or groups, form the basis for potential conflict (Walsham, 2002). While contradictions are an expression of the main “fault lines” of societal and cultural differences (Giddens, 1984, p. 198), conflict is the actual struggle between individuals and groups. According to Giddens (1984), contradictions invariably lead to conflict.

Furthermore, information security researchers have established that differences in values held by groups and individuals inevitably lead to conflict, which in turn has a negative influence on information security compliance behaviour (Kolkowska, 2011; Hedström et al., 2011; Karlsson et al., 2018). Contradictions, resulting in conflict can therefore lead to non-compliant behaviour by those deeming the required adjustment practices to affect them negatively. As Giddens (1984) argued, conflict arises when an actor feels a contradiction will impact them negatively.

The notion of contradictions as the basis for conflict (Walsham, 2002), and the subsequent negative influence it has on compliance behaviour was corroborated in an analysis of the data collected. Most participants who expressed a degree of frustration, and who viewed information security as a hindrance, also explained how this leads them to evade ISPs. For example, a systems analyst explained how an information security process hindered them from sharing important project information with vendors in a timeous manner. They therefore decided to develop their own workarounds by bypassing an authorised information security channel, and put an alternative solution in place instead, which was an unintended consequence of ISPs:

So we need to share information with a third party vendors...What is very restricted for us at the moment is that we can't share information with them... So what we've done was, we've decided that we will set up a OneDrive site for them...So we have to go through a whole process of federating with their domain, and then like sort of a month later, we can, you know, share information with them and stuff like that, you

know. So that delays the process...So that's one thing that actually hinders the project a lot and possibly delay us. So it does impede on productivity or efficiently.

Similarly, a senior technical specialist expressed the difficulty in remembering multiple passwords as part of the organisation's password complexity policy, and therefore resorted to saving passwords in an unencrypted text file:

I think your password complexity is one of the policies that should be enforced...We've got so many passwords. The problem with that is remembering those passwords, and in doing that you might even, sort of, I don't know if maybe breaches is too strong a word, because you save these passwords maybe in a text form that you can just remember then.

Most participants who experienced contradictions, and who perceived information security as hindering their performance, also explained how they were invariably inclined to non-compliant behaviour. The same behaviour was also observed by an IT manager:

There're a lot of people who don't comply, but not intentionally. And all they're doing is they're wanting to get things done, so that's why they don't comply, because they're not any the wiser and all they're thinking is I'm doing my job.

This behavioural pattern of contradictions, leading to conflict, which leads to non-compliant behaviour was also experienced among information security personnel. An information security specialist explained how a contradiction in information security processes sometimes led to conflicting feelings of needing to get the job done regardless of the policy in question:

Yes, that wasn't in line with policy, yes. And then, and I think it's always in the back of my mind. I think. OK, that's probably not the right thing to do. But I still need to do it because I know what the policy is.

It is evident from the data collected in this study, that participants indeed believed that ISPs were impacting their performance and efficiency in a negative manner. This was consistent with Structuration Theory which posits that conflict occurs as result of contradictions affecting actors negatively (Walsham, 2002). The data also confirms that conflict, leading to non-compliant behaviour, is evident with the emergence of Priority Contradictions, Process Contradictions, Technology Contradictions, and Vision Contradictions.

It has also been established that the organisation had an orientation towards cultural values of innovation and goal achievement, as discussed in section 5.3. Information security priorities, processes, technology, and goals are therefore oftentimes in contradiction with the organisation's primary cultural values of innovation and goal achievement. This was evidenced by the feelings of frustration of employees that ISPs were impeding their productivity and performance. Consistent with literature, Van Niekerk and Von Solms (2010) pointed out that the goal of securing information most often conflicts with the organisational goal of business productivity and efficiency, which is validated by the data collected in this study.

The secondary research question has therefore been addressed in identifying the cultural contradictions that emerged in the information security compliance behaviour of employees. The analysis has also confirmed that emerging contradictions can result in conflict, which lead to actual action of non-compliance to ISPs. Following is an analysis of the social structures of information security.

5.5 Structurational Analysis

This section endeavoured to further interrogate the emerging themes from the previous section of cultural contradictions, conflict, and information security compliance behaviour. Having achieved the first research objective of identifying cultural contradictions, the goal of this section was to attain the second research objective, by examining how cultural contradictions influence the information security compliance behaviour of employees.

The structural analysis used a synthesised adaptation of Structuration Theory (Walsham, 2002; Bernardi, 2017) as a sensitising lens to trace the process of structuration, as outlined in the proposed theoretical framework. The three structures to be examined are meaning constitution (Signification), forms of power (Domination), and normative behaviour (Legitimation). Actors draw on their stocks of knowledge [interpretive schemes] in order to make sense of their actions and the actions of others (Walsham & Han, 1990), which in turn produce and reproduce structures of signification (Giddens, 1984). Authoritative and allocative resources form the basis for exercising power [facilities], which (re)produce structures of domination (Giddens, 1979). Social actors also draw upon socially acceptable conduct [norms] and standards of morality in order to sanction their own actions thereby producing and reproducing structures of legitimation (Walsham & Han, 1990).

It is pertinent to reiterate that structures are separable only analytically. Structures of signification, domination and legitimation are intricately linked in reality (Giddens, 1979). To illustrate, the case data presented a discrepancy between the expected compliance behaviour of employees and the existing structures of signification. The expected information security compliance behaviour was related to sets of norms, which constitute structures of legitimation. While the organisation expected sanctioned behaviour to comply with ISPs in accordance with structures of legitimation, the actual interpretive schemes communicated through awareness programmes were limited to cyber security policies, which constitute structures of signification. This indicated a possible misalignment between structures of signification and the expected structures of legitimation. Bernardi (2017), in studying the implications of accountability in structuration processes, argued that the alignment of structures was necessary for accountability to be legitimised. In this case study, it could be argued, the alignment of structures of signification, domination and legitimation is necessary for desirable information security compliance behaviour to be realised.

5.5.1 Information Security and Structures of Signification

This section seeks to analyse how institutionalised properties of interpretive schemes in the social domain mutually shape ISP features in the technology domain, and the cultural contradictions that emerge in signification structures. Structures of signification essentially inform, and are informed by, systems of meaning or interpretive schemes, which represent institutionalised rules communicated to actors in interaction (Orlikowski, 1992). Interpretive schemes are embedded in information security features of IS within the technology domain, as well as the stocks of knowledge within the social domain, that individuals draw upon as they interact with technology (Walsham, 2011). ISPs are a means of providing employees with a necessary interpretive scheme of information security to draw upon (Arhin & Wiredu, 2018).

There appeared to be an established interpretive scheme or system of meaning pertaining to information security for users to draw upon in interaction. Most participants, in expressing their interpretation of the role of information security, understood the cardinal goal to be about securing information, whether personal or organisational. As an IT manager responded to his view on the role of information security, “In my view, I think it's protecting organisation's data as such in an IT environment. We've also got our information sitting with like the HR department, and I think it's protecting that information as well”. A similar

interpretation of the role of information security was widely held by most participants. As a SAP real estate master data specialist explained, “To protect their company’s information and to make sure that the integrity is intact”. Based on research, these are good interpretations of the role of information security (Van Niekerk & Von Solms, 2010). This was largely due to the organisation’s information security awareness program. Security training is a means of increasing security awareness (Van Niekerk & Von Solms, 2010), which also informs interpretive schemes and reinforces structures of signification. The communication of espoused interpretive schemes, such as ISPs, is a way for the organisation to produce and reproduce desirable information security structures of signification (Arhin & Wiredu, 2018).

5.5.1.1 Information Security Goals and Interpretive Schemes

ISPs, which comprise embedded elements of interpretive schemes and expected norms, appeared to be a collaborative effort between the information security team and management. For example, when asked whether ISPs are an information security team or management initiative, an advanced analytics and assurance specialist explained:

I think, it comes from the Board, then it filters down to senior management and middle management. So, I would say, I think, it is part cybersecurity guys, but I think, it is also part of the management structures at ORG₁.

Similarly, a technical analyst believed it was a collaborative effort: “I think it's both, because as a security person, you also need to drive the initiatives in the business”. An IT manager had a similar view and explained that top management had an overall awareness, but still depended on the input of information security personnel current risks:

Okay so there’s definitely an awareness at top level management... I think it’s a two-way thing and it’s really for the people at the bottom to understand these things, to be reporting the correct things through to management so that they have that insight and visibility of what’s going on to fund the project that you require. So it can be driven from the top down as well.

This indicated that the security team was a chief motivator in the organisation’s espoused interpretive schemes of security that were embedded in IS, and by implication, the information security structures of signification. As discovered in analysing the data for Vision Contradictions, the goals of information security personnel were indeed aligned with

the information security goals of the organisation. Furthermore, the finding also implicated structures of domination, as the information security team mobilised resources to facilitate power in the social domain over ISPs in the technology domain. Thus, information security personnel, through the deployment of resources, had the power to shape ISPs in the technology domain, and thereby influenced the organisation's signification and legitimisation structures.

5.5.1.2 Misalignment of Goals with Non-Security Personnel

This study found evidence of Vision Contradictions, as outlined in section 5.4.4. Although the information security goals of the organisational leadership and information security personnel were aligned, evidence suggested that non-security personnel were unaware of those goals, which had a negative impact on compliance behaviour (Guo et al., 2011). For example, when asked if participants were aware of the organisation's information security goals, two technical analysts answered respectively, "I'm not aware to be honest with you of any information security goals", and "there's no transparency from them, exactly as to what their roadmap is...So we are just told, look we implemented this...We just find out it's been implemented". Likewise, a service desk specialist reiterated the same, "In terms of goals, no. I am not aware of that". This led to a misalignment in information security goals between non-security personnel and the organisation.

This implies that the interpretive schemes that individuals draw upon in compliance behaviour diverged from the systems of meanings about information security purported by the organisation. This disparity in structural principles, according to Giddens (1984), forms the basis for contradictions, which inevitably breed conflict. The interests of different groups must align for an organisation to realise a common goal of commitment to information security compliance (Tsohou, Karyda, Kokolakis, & Kiountouzis, 2015; Bernardi, 2017). This alignment is a challenge if individuals lack an understanding of the organisation's security goals and, in effect, the espoused interpretive schemes and expected norms. Non-security personnel had no knowledge of the organisation's information security goals. This indicated a misalignment of information security interests between groups, which led to contradictions in interpretive schemes and norms in the social domain, which informed how employees interpret information security features in the technology domain. An unintended consequence of these apparent contradictions was the production of misaligned structures of signification and legitimisation. In addition, a lack of understanding of information security

goals further amplified the effects of Priority Contradictions, as employees would likely prioritise their own goals over ISPs (Adams & Sasse, 1999; Parsons et al., 2014).

Furthermore, where interpretive schemes for ISPs are lacking and misaligned, individuals will place a greater reliance on their knowledge and the reflexive monitoring of the consequences of their own actions, and the actions of others (Bernardi, 2017). It is also posited that where relevant stocks of knowledge and interpretive schemes are lacking, individuals will revert to generalisations and stereotypes to inform their actions (Festing & Maletzky, 2011). Users were therefore in a sense left to themselves to make sense of the information security world around them. There were also suggestions of negative perceptions of information security personnel, or stereotypes, which non-security personnel drew upon in the event of contradictions. A technical analyst expressed:

Because the security team get seen almost as this bureaucratic department now that like to enforce like their will on you...it's easy to get into the mindset of, you know what, I'm just going to do whatever I want to do, because you're forcing me now to do extra work, you're forcing me not to do extra things, and you're forcing me now to do things that I wasn't doing before.

Analysis of results therefore showed evidence that individuals hold meanings and perceptions of information security, and security professionals in particular, that were antithetic to the organisation's information security goals.

5.5.2 Information Security and Structures of Domination

The aim of this section was to link the implementation of ISPs to structures of domination and analyse potential contradictions that emerge. According to Giddens (1984), power over resources take two distinguishing forms, namely power over allocative resources and power over authoritative resources. Allocative resources refer to control over material objects, while authoritative resources refer to command over people or actors (Jones & Karsten, 2008).

Arhin and Wiredu (2018) argue that organisations can exercise power and sustain managerial control by implementing ISPs. ISPs are therefore a means of exercising organisational power by communicating the espoused interpretive schemes of security, and sanctioning unacceptable compliance behaviour. The following data extracts from a senior SAP basis specialist confirmed this notion, as most employees in this case study believed the

organisation had the power to apply punitive actions if ISPs were not adhered to: “if you are not compliant and you are overstepping something, you know what I mean, in that space itself, I think disciplinary action needs to be taken”. Likewise, a solution specialist and a systems analyst shared the same view:

For that question, I think it's very reasonable. Because our company has driven an information security awareness campaign last year or the year before. Excuse me. It was compulsory for everyone to complete this training. So no one can deny the fact that he or she did not know of information security...I think it's very reasonable because there is no excuse.

Yeah, for sure...There is sort of information security training and stuff that they frequently do, and that is compulsory for the employees to do. So, if we breach those policies, I think...the company is within their right to discipline their employees for breach of policy.

Most participants who believed the organisation had the power to discipline non-compliant behaviour, also added a caveat that disciplinary actions should be reasonable and befitting the behaviour. For example, a senior SAP basis specialist added, “It is not necessary that you need to fire the person, but it depends on what was breached as well”. Similarly, a security specialist and an advanced analytics and assurance specialist believed the organisation had the right to take corrective action for non-compliant behaviour, as long as it's reasonable:

it is actually two fundamentally different use cases. Unknowingly means it is a human error...I do not believe that it is right to punish a person for a human error. We are people, we make mistakes, right...if it is a mistake, I do not believe punishing people will have your desired outcomes. It could be more detrimental for you. If someone is violating your policy in a malicious manner...In that case, I believe that consequence management is the way to go. Whether it is firing him, whether it is taking criminal charges against him, but if you with certainty know their intention was malicious, then yes, you need to act on it.

Although most participants believed the organisation had the right to discipline an employee who violates a policy, albeit within reason, some placed the responsibility for non-compliant behaviour with the organisation. This view was expressed by management, IS professionals

and business users alike. Reasons for this view are mapped in Figure 6 below, with accompanying data extracts per theme outlined in Table 7.

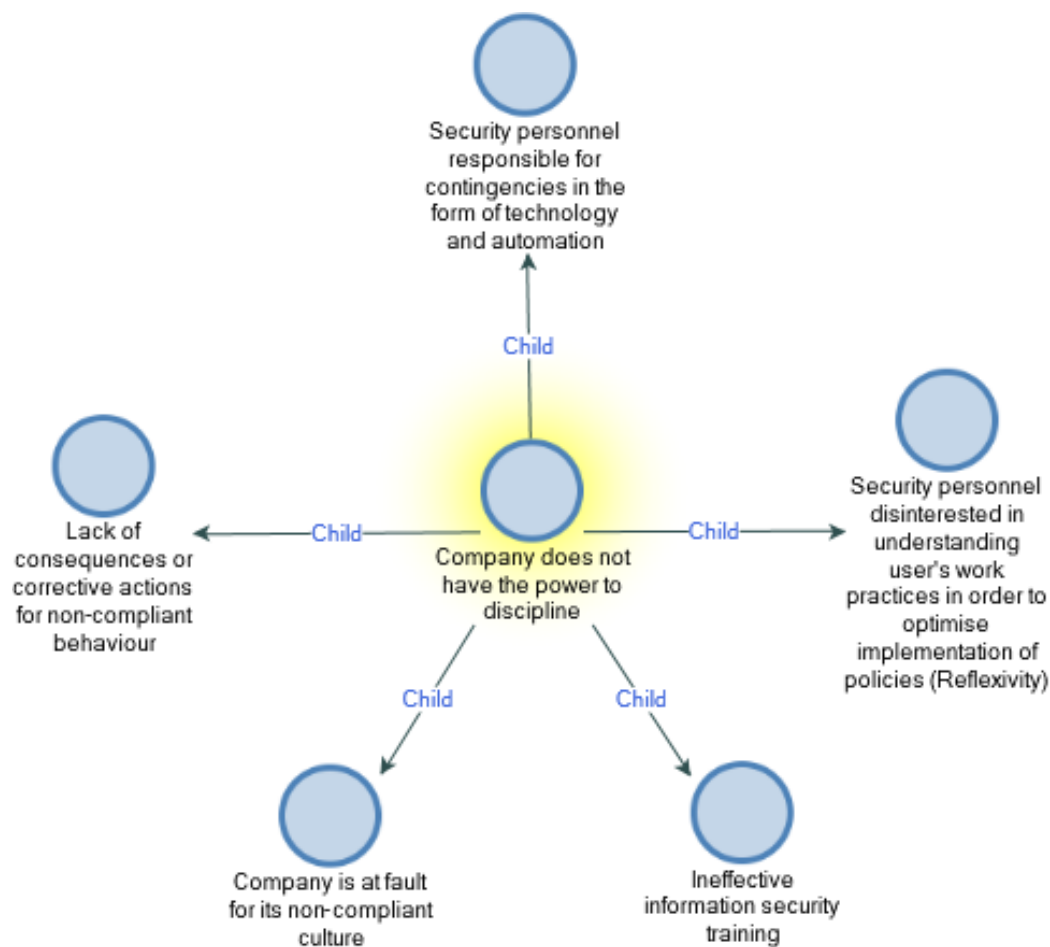


Figure 6. Employee Views of Power and Sanctions

Table 7. Employee Views of Power and Sanctions Data Extracts

Sub-Themes	Data Extract	Ref.
Company is at fault for its non-compliant culture.	“I think there needs to be leniency because at the end of the day it’s the organisation that’s at fault and it’s the culture of the organisation at fault.”	IPT14
Ineffective information security training.	“I would say no. My reason being, in saying no. Just like, I don't think, as a company, we are, from security or HR, there's enough information being spread out to people about warning them about such things. There is few trainings, but really, like you look at it like once a year. It's not enough.”	IPT8

Lack of consequences or corrective actions for non-compliant behaviour.	“The biggest problem is, I don't think that people understand the consequences of not following that policy. And possibly, if people were taught or exposed to the consequences of not being circumspect with company information, then possibly less of it would happen”	IPT7
Security personnel uninterested in understanding user's work practices to optimise implementation of policies (Reflexivity).	“most times it's a one size fits all policy that gets blanketed out or copied and pasted...I think it's more beneficial if you ask that person, so how did you get phished, what was your thinking process around it, what happened to you, as opposed to just putting stats and saying oh we phished 50 people and 30 people clicked on the link, but they have no understanding of why the person did it or how he got to that point, what was he busy doing...let's have a talk about this like I see this is what happened, how did you get to that point, what ... you know, as opposed to just now you're just blanketing another okay, you need to go on training now because you got phished like recognised.”	IPT13
Security personnel responsible for contingencies in the form of technology and automation.	“No. The company has all the technology that can provide an extra buffer for the employees. I would think that the employees can actually sue the company because you are not providing me that security. You should provide that for me...I think that there is a bit of a case there for whoever gets penalised regarding that. You can just argue that you had the technology. Are you utilising technology?”	IPT9

This evidence demonstrates that structures of domination should not be conceptualised as only having a constraining effect on actors, but that individuals also have the autonomy to resist and exercise a degree of power over the reproduction of their social systems (Giddens, 1979). Power is therefore a two-way relation referred to as the “dialectic of control” (Giddens, 1984, p. 16), where social actors can act against institutionalised artefacts determined by the organisation, such as ISPs (Orlikowski, 1992). The extracted responses in Table 7 illustrated this dialectic of control, where subordinates expressed a form of resistance to potential sanctions against information security non-compliant behaviour. Similarly, Walsham (2002) found users exercising power over their superiors by passively resisting the use of a new information system.

All sanctions, regardless of how beneficial or oppressive, are still dependent on the acquiescence of social actions (Jones & Karsten, 2008). Regardless of the comprehensiveness of ISPs in structures of signification, and their associated sanctions in structures of legitimation, individuals still have the power to adhere to or violate those policies. This was evinced by the observation that information security non-compliant behaviour of employees within this case study was common. Actors can therefore choose their own response to ISPs, which is inherently characteristic of structures of domination and the dialectic of control.

This finding indicated contradictory views on power as it relates to sanctions. Most employees believed the organisation was within its right to discipline information security non-compliant behaviour within reason. Some however cited reasons for believing the organisation wouldn't be justified for punishing an employee for information security non-compliant behaviour.

5.5.2.1 Information Security Training as a Facility

Organisations can use training and awareness programmes as a resource to facilitate the communication of security interpretive schemes, with the intended consequence of producing and reproducing desired information security structures of signification (Arhin & Wiredu, 2018). Training and awareness programmes serve as a means of increasing stocks of knowledge about ISPs (Ifinedo, 2012), which is also the modality of structuration which actors drawn upon in the communication of interpretive schemes. Furthermore, through forms of training, organisations can facilitate the conveyance of behavioural expectations, with the intended consequence of sanctioning conduct which produces and reproduces legitimation structures. The organisation therefore exercised power by using a Cyber Security Training programme as a facility to communicate intended interpretive schemes and increase employee stocks of knowledge about information security, while also sanctioning negative security behaviour. Security and awareness training therefore shaped how employees interpreted and interacted with ISPs and features in the technology domain, which ultimately had implications on structures of signification, domination, and legitimation.

The organisation also conducted targeted security simulations as part of the Cyber Security Training programme, such as phishing email simulations. Employees who failed these simulations were typically sanctioned to attend additional security awareness training. As a technical analyst shared "Except, if you click on that phishing email by accident then they

send you on that training again”, which was also the organisation’s means of exercising power. Employees also expressed a sense of embarrassment for failing a phishing simulation, which indicates a degree of reflexive monitoring on the part of employees. Awareness programs, such as the Cyber Security Training, can be a means of communicating interpretive schemes and producing desired structures of signification.

5.5.2.1.1 Security Training as a Facility of Interpretive Schemes and Norms

Increasing knowledge of ISPs is an effective means of increasing awareness (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014), which serves to produce and reproduce desired structures of signification and legitimation (Arhin & Wiredu, 2018). However, increased awareness does not always translate into compliance behaviour, as is evident in this case study, which was an unintended consequence of the organisation’s awareness training programme.

The nature of the organisation’s training and phishing content could be a possible reason for the ineffectiveness of the awareness programme. The training and phishing simulations appeared to focus primarily on cyber security, which can be defined as the protection of information on the internet (von Solms & von Solms, 2018). An analysis of the content covered in the Cyber Security Training and phishing simulation program showed little consideration for information security, which is the protection of information everywhere (von Solms & von Solms, 2018). The overall topics covered by the Cyber Security Training program and phishing simulations were all within the scope of cyber security. The Cyber Security Training themes were:

- Phishing
- Social Media
- Privilege Identity
- Personal Information at work
- Gamification training

Perhaps coincidental, but the term used for the awareness programme alluded to its emphasis. In addition, a crucial part of the Cyber Security Training programme was its phishing simulations. Phishing is essentially classified as a cyber-related risk (von Solms & von Solms, 2018). As an advanced analytics and assurance specialist, and a principal solution

design specialist pointed out, “We have simulations like phishing exercises and things, but I feel the company never tells the why”, “When I look at the ORG₂ stuff, it is more just phishing training to me, or that cyber training”. Similarly, a security specialist explained “we don't really look at...at information security. We look more at cybersecurity, and we put information security under the Cyber Security umbrella”. An IT manager expressed similar views about the nature of the Cyber Security Training content:

And we're great at driving phishing and cyber security risk of people stealing your information and identities and getting access to information so we've been great in that in the past year or two, but haven't been great in terms of creating awareness around information and management of information, you know there's still people printing a lot of stuff off and just leaving it all over the show in hard copy format information and people have access to it, contracts, vending information.

Evidently, while the organisation's awareness program has contributed positively towards providing employees with an interpretive scheme for cyber security related risks, such as the protection of information on the internet, it was still lacking in producing interpretive schemes which encompasses the protection of information assets everywhere. This distinction is elaborated on by Von Solms and Von Solms (2018) who define cyber security as a part of information security. A security specialist alluded to this fact when stating:

It's an area that's being overlooked. I mean, it's only now that Protection of Personal Information Act (POPIA) is here, and it's enforced, and it's law and all that kind of stuff, that companies like ORG₁ is really looking into how do we protect our data. And are people adhering to our policies? I mean, how is the data being shared and all that kind of stuff you know?

Although adequate for cyber security awareness, the training programme as a resource therefore communicated rules that are devoid of broader information security interpretive schemes and norms. This ultimately shaped how employees interact and interpret information security in the technology domain.

5.5.2.1.2 Security Awareness Training Informing Sanctions

Furthermore, some participants believed the training was insufficient as it is failed to explicate the possible consequences of non-compliant behaviour. This had implications on

norms or right conduct that is sanctioned through structures of legitimation. As an advanced analytics and assurance specialist from the audit team explained:

We have simulations like phishing exercises and things, but I feel the company never tells the why. It is just like, we need to protect it and go through this exercise and make sure you get 100%. But the why, you know, to inform the users...“This is why we should not share information. This is what happens if different information is shared, and the consequences of it, as well. This could bring the company in disrepute. We can lose financially.” People do not know these things. Most people do not know.

A security specialist perceived the same limitation of the Cyber Security Training programme: “You see, if you do not start with the ‘why’, right, you are going to have people seeing your training as ineffective”. The organisation’s Cyber Security Training programme can be an effective resource to facilitate the communication of information security related interpretive schemes and norms in the social domain. The intended consequence of an effective training programme should be to shape how employees use and interpret technology and its security policies in the technology domain, and thereby produce desired structures of signification and legitimation. However, the organisation’s awareness training programme appeared to be limited in its content. The training material seldom explained the consequences of not complying to ISPs, and thereby communicating why compliance behaviour is important. Furthermore, the content had a strong emphasis towards cyber security and the protection of information on the internet, with little content addressing the safeguarding of information in general.

5.5.2.2 Power Over Authoritative Resources

Most participants believed that ISPs are a collaborative effort between management and the information security team, as shown by the following data extracts from the transcripts of an advanced analytics and assurance specialist, and a security specialist: “So, I would say, I think, it is part cybersecurity guys, but I think, it is also part of the Management structures at ORG₁”, “So, I think, information security should be driven by the business and then enforced by the information security department, yeah”. Likewise, a delivery claims investigator said:

I would think, maybe from a security team or department, this probably also gets somehow motivated to top management to make that decision. Because ultimately,

they are the core of what, you know, is the pain points, and what is the next steps to try and, you know, eradicate these you know.

Additionally, a senior integration architect explained how the security team exercised authoritative power over ISPs decisions:

And honestly, sometimes I will be quite frank with you, I think it is an ego thing with certain people. And it is not just for the ORG₁ security guys, it is broadly speaking, I hold this power over you, and therefore, I am going to flex my ego, and that is often the case as well and, that does not ultimately bode well, from a compliance point of view.

ISP implementations were therefore a collaborative effort between management and information security personnel. Furthermore, the data revealed a strong influence from the organisation's parent company ORG₂ on its information security goals and initiatives. This unexpected theme implied that ORG₂ had the authoritative power to exercise a degree of control over the ISPs and features within the technology domain at ORG₁. As an advanced analytics and assurance specialist explained, "I have seen more and more over the years where ORG₂ was, I do not want to say on the sidelines, but their operational processes, their strategic goals have now become ORG₁'s strategic goals". The sentiments were reiterated by a senior technical specialist:

Yes, I think I think they do have security goals, which is companywide, is to make sure that all company information is protected, and in those of the employees. And I think, coming from our parent company, they do. And they're very, I'm not sure if they're strict about it, but it's quite a high priority with them, with information protection, and company's information and systems.

Likewise, a principal solution design specialist said, "No. I see management being put under pressure by ORG₂...ORG₂ puts pressure on ORG₁, and then they put pressure on the employees. But it is also a thing of being scared of the, you know, the parent company". This was echoed by an IT manager:

to be honest I don't think we have security guys who think like that. They're just accepting what's coming their way and ORG₂ is saying they don't even care what you have and then they want to put in solutions. It doesn't work that way.

The CIO and an IT manager justified this structural property and explained that the two organisations were essentially trying to address the same information security risks, albeit in different national contexts:

So I think the stuff that is driven from ORG₂'s side is nothing new, it's something that's been on our radar for the past 10 years. I think we're all more or less at the same stage here so what we're trying to drive now ORG₂ is trying to drive as well...I think that is important, is that every organisation is the same. We all have the same challenges, we're just different levels of maturity so I don't think we're unique. We think we are unique but we're all the same, you know when you're part of a bigger corporate, you're going to have the same challenges.

We are very far away so therefore we can have certain tweaks and triggers that are different because we are in a different geography. We are in a different country, we are in different legislative environments, etcetera, etcetera...that does not mean that you can compromise on the culture of saying I need to have a high level of awareness where any risk is introduced to the organisation. Whether that is going to be related to financial risk or to any business risk or reputational damage or, anything like that. So, in essence, your high-level behaviours should be the same and should be consistent.

This added further complexity to the structuration process as there were definitive contextual and cultural differences between ORG₁ and ORG₂, which also implied inevitable differences in social structures. There were differences in national cultures, as ORG₁ was in sub-Saharan Africa and ORG₂ was in the southeast Asian region. The less powerful in Asian countries generally have a higher acceptance of unevenly distributed power than in sub-Saharan African countries (Hofstede, Hofstede, & Minkov, 2010). Asian organisations therefore have a stronger social hierarchy than sub-Saharan African organisations, which has implications on how the two organisations view power and facilities in structures of domination. Secondly, ORG₁ was a privately owned organisation, whereas ORG₂ was wholly government owned and operated as a parastatal organisation. As the IT manager explained further:

There are major cultural differences between ORG₁ and ORG₂... But it's difficult, we're in a sort of... it's a global divide between the two of us, between sub-Saharan Africa and Asia and with them being an Asian national company and us being an independent within South Africa, owned by an Asian national company. So it brings all different dynamics in terms of your operations. ORG₁ has always been, we haven't been run like a parastatal, but ORG₂ is ...that's the way they run or operate. Their hierarchical structures and everything else is based on that...And I know that sometimes it feels that the ORG₂, they want to dictate to us and we feel we know better.

Given the differences in national and organisational cultures, the two organisations appeared to have contradictory views on facilities through which power is exercised. Furthermore, in an interrogation of organisational culture, this study established that ORG₁ had a cultural orientation of goal setting and innovation. This was expected to differ from ORG₂'s cultural orientation which, by virtue of it being a parastatal organisation, had a strong rule orientation. As Cameron and Quinn, (2011) argued, "Large organizations and government agencies are generally dominated by a hierarchy culture" (Cameron & Quinn, 2011, p. 38), with an emphasis on enforcing rules. Moreover, a hierarchical and rule based cultural orientation is likely to be endorsed by institutional members where there is a strong social hierarchy with strong acceptance of unevenly distributed power, as was the case with ORG₂. However, the opposite seemed to be the case for ORG₁, which was not rule orientated and did not measure as high in acceptance of unevenly distributed power. This was evident by some of the observations of participants, where there was a sense that initiatives in the technology domain, and the social domain, were forced upon the information security team, regardless of differing objections. A security specialist shared:

I think it's getting to a point where you're kind of being told what to do. And where I'm going with this is, so our parent company, ORG₂, and this is from a security point of view. We starting to get a lot of directives from them. How we should implement stuff. And what we need to implement, and how we need to implement it, so we don't really have a say as to what needs to be implemented, how it needs to be implemented, and what policies etc. No, those things are just pushed down, so it's becoming more of a top down.

A senior technical specialist shared the same views: “I do have that sense yes, it is coming from the very top. Even coming from our parent company. They're pushing it quite rigorously”, as well as a technical analyst:

Absolutely, I mean even when we were given the Identity Access Management (IAM) notice, you almost felt like you're being included here simply to make you aware of it as opposed to being included in it to actually get your input in it. So they've, I mean our security team were given almost their marching orders from the head office, who uses IAM. And they sit in a country outside of South Africa, and so they're using it and they've found some success in it. And now to standardise, they've basically pushed that through to all the companies that they own.

This highlighted potential contradictions in domination structures, where ORG₁ personnel felt information security goals, initiatives and policies were imposed upon them by ORG₂. While structural analysis showed that the information security team shares interpretive schemes and signification structures with management, these interpretive schemes were to an extent involuntarily exacted upon them. This could partly explain why all employees experienced contradictions in priorities, processes and technology, as illustrated by the data extracts in Table 8. Furthermore, these contradictions did indeed lead to conflict, as was evident by the information security non-compliant behaviour observed among all employees, including management. This confirms that the contradictions experienced by all employees can indeed lead to conflict (Walsham, 2002), and resistance to ISPs, expressed as non-compliant behaviour.

Table 8. Contradictions Among Information Security Personnel.

Contradiction	Data Extract	Ref.
Priority	“I think it should be flexible. If I can call it that. Because if you go with a policy that is so rigid. That you can't...there's no scope to move a little bit away from that policy. Then, you know it's going to cause a lot of...and then...and I think in in terms of productivity, and you see it a lot...But then...you know but, people break policies all the time.”	IPT1
Process	“Yes, that wasn't in line with policy, yes. And then, and I think it's always in the back of my mind. I think. OK, that's probably not the right thing to do. But I still need to do	IPT1

	it because I know what the policy is. But I need to do this thing, you know. And...and then it's a bit of a conflict because you want people to adhere to cyber security and information security and you're kind of breaking that...So, for me breaking policy it, it's not really a good thing and I don't really like it, but sometimes I do.”	
Technology	“Let us say you implement a solution like IAM. Now as a support person you have your way of doing support and it works for you, right. Now we are putting a layer of security in and it is changing the way you log on...That is the type of stuff that results in security being seen in a bad light...So yes, I have seen situations where we have amended or changed the business process to introduce security. In some cases, the changes are small enough and I am in agreement with it. In other cases, I do not believe it is the right way of doing it, because business users, when you start asking people to change things, that is where you start getting resistance.”	IPT15

In addition to ORG₂ mobilising facilities to exercise power over information security features within the technology domain, the parent organisation also exerted a form of power over the expected normative behaviour of ORG₁ employees within the social domain. Secondary data analysis showed that in 2014 the organisation actively embarked on an initiative to replicate ORG₂'s new cultural beliefs on their subsidiary, with the aim of producing uniformity in cultural values. A 2018 newsletter sent to ORG₁ employees summarised the implementation of the shared cultural values:

In November 2014, leaders from across ORG₂ subsidiaries and ORG₁ identified a list of current beliefs that were getting in the way of achieving desired results. These beliefs included silo mentality, leaders not walking the talk, lack of transparency in communication, employees not being open to giving or receiving feedback.

The effort to replicate ORG₂'s shared cultural beliefs to ORG₁ was reflected in newsletters, reiterating the importance of living the shared cultural values, “We must therefore all continue to focus on living our shared values and enacting the ORG₂ Cultural Beliefs”. The parent organisation was evidently using information security features and cultural beliefs as facilities to exercise control over the technology domain and social domain at ORG₁. However, despite their best efforts to create a uniform culture, there remained unassailable cultural differences between the organisations. An IT manager with 30 years of service

confirms “There are major cultural differences between ORG₁ and ORG₂, even though we don’t want to believe that and we’re trying to have one culture across the organisation”.

5.5.2.3 Power Over Allocative Resources

Funding, which Giddens (1979) classified as a form of allocative resources, is necessary to implement ISPs, which is ultimately controlled by management (Da Veiga & Eloff, 2010; AlHogail, 2015). In order to obtain funding for their initiatives, the information security team had to legitimise ISPs with management. Thus, by legitimising their information security initiatives, information security personnel obtained funding to implement new ISPs in the technology domain, and thereby influenced interpretive schemes and acceptable norms in the social domain. As an IT manager who was partly responsible for approving procurement requests explained:

So you're not going to get funding for programmes if you try and hide things or you report things incorrectly...So it's important to actually to ensure that you get the right funding for your initiatives by reporting correctly and it's a two way thing.

Information security personnel therefore drew upon their own skills, reports, and industry recommendations from vendors and experts, to influence the deployment of allocative resources towards their initiatives in structures of domination.

5.5.3 Information Security and Structures of Legitimation

The following section aimed to analyse the information security compliance behaviour of employees through the lens of legitimation structures. Structures of legitimation are the structural properties of normative regulations which actors draw upon in social interactions (Giddens, 1984). In this study normative regulations refer to the expected compliance behaviour, as defined by ISPs in structures of signification. While structures of signification comprise rules in the constitution of meaning, structures of legitimation encompass the rules or principles of normative conduct (Walsham, 2002), which in this study, is information security conduct. ISPs are intended to guide the normal security behaviour of employees and hold them accountable for their actions (Cram et al., 2017).

5.5.3.1 Modality of Normative Compliance Behaviour

Participants experienced an increase in information security awareness because of the organisation's Cyber Security Training. However, of relevance to structures of legitimation is whether the increase in awareness leads to the intended consequence of an increase in normative behaviour of security compliance. The data showed that the actual norms of employees resembled a degree of non-compliance towards ISPs. That is, the institutionalised or individualised interpretive schemes and norms in the social domain shaped employee use of technology in the technology domain in a non-compliant manner. This could partly be due to the nature of the Cyber Security Training content, which was limited to meanings of cyber security only. This has been elaborated in the analysis of domination structures in section 4.5.2.

5.5.3.2 The Modality of Information Security Compliance Norms and Sanctions

Despite the notable increase in information security risk awareness, shown in Table 5, participants still noted a prevailing behaviour of non-compliance among employees and management alike, as discussed in section 5.2. Moreover, there was evidence that cultural contradictions did indeed lead to conflict, resulting in information security non-compliance behaviour, as discussed in section 5.4. By the security team's own admission, contradictions between ISPs in the technology domain, and the performance goals of the organisation and its members in the social domain, conflicted and led to non-compliant behaviour. As two security specialists stated:

I have observed it, yes...And it is normally coming from, it is all coming from the same place. People have got deliverables, they have got KPIs, they have got deadlines, right...No, definitely across all levels, because remember ultimately, you have got you implementers that is executing on the mandate of the manager.

Information security and cyber security is more a nuisance, for I would say 90% of the people in the company...And in some cases, it does slow down productivity... They got to do cyber security training. They get to do all these things, and then I guarantee you, and that is based on what we can see when we do cyber security campaigns.

Although the security team was communicating security risks to top management, with the help of industry knowledge experts and ORG₂, thus establishing new interpretive schemes and structures of signification which supported strict security governance, there was still a lack of emphasis on enforcing compliance behaviour to new and existing interpretive schemes. That is, while information security rules in the constitution of meaning were articulated to employees in the social domain, associated rules which constituted acceptable conduct were not communicated. Evidence therefore suggested that while ISPs were formally defined in interpretive schemes, sanctions against non-compliant behaviour were however not enforced. For example, a security analyst explained that ISPs were seldom enforced through sanctions:

I haven't heard of anybody, that's where sanctions have been issued to an individual, who for instance, copied a document or shared a document. You will hear about for instance, an email was sent out to a news outlet or paper. And then you are asked to investigate who leaked the information...I mean, I don't know about anybody that's been sanctioned or reprimanded because of that.

An IT manager echoed the same observations:

And ORG₁ has always been a company where we have ... where we are not very punitive around how we deal with ORG₁ consequence management. So, that is where we came from... So, they want to get to that stage where we do take these things seriously and there's punitive measures in place when people do not adhere to it.

The CIO confirmed the same: "We have people that have been caught five times in a row and have not even had a disciplinary discussion". That is, the unexpected consequence of weak sanctions on deviant normative behaviour in the social domain, was the adverse shaping of employee use of IS in the technology domain. The following data extract of a senior integration architect's view on ORG₁'s policy enforcement, illustrated the misalignment between information security interpretive schemes and weakly sanctioned deviant norms.

They will make the strictest policy, but they will not enforce it unless the day they want to, then it is available to them. Again, the trust, and everything goes out of the window there, because then you get people who are just not willing to do things for

the company, as an example, or going out of their way...So, you are going to discourage potentially a lot of value adding activities.

5.5.3.2.1 Lack of Consequences for Non-Compliant Behaviour

A lack of ISP enforcement through sanctions also led to a corresponding lack of consequence management. This was a developing theme in structurational analysis, where participants generally bemoaned the lack of consequence management for information security non-compliant behaviour. Similarly, legitimisation structures implicated a lack of consequence management in information security compliance norms in the social domain. A SAP real estate master data specialist explained that the organisation generally did not take disciplinary action against non-compliant behaviour:

One of the biggest problems I find in ORG₁ is that there is no accountability...There's consequences...A written warning that will sit on your file for a year, and if you do it again within that year you will be fired. The end.

A security specialist shared the same observations: "I don't know about anybody that that's being sanctioned or reprimanded because of that", which was corroborated by an IT manager:

And ORG₁ has always been a company where we have ... where we are not very punitive around how we deal with ORG₁ consequence management...So, when it comes to information security and people not doing the right things, we are forgiving about it.

The structuration concept of the knowledgeability of social actors means human beings reflexively monitor their actions and the actions of others (Orlikowski, 1992). That is, individuals will reflexively monitor the intended and unintended consequences of actions taken by human beings. If the consequences of human action taken is viewed as negative, then it is unlikely that the individual will follow the same action in similar circumstances (Walsham, 2002). Weakly enforced sanctions and lack of consequences clearly contribute to the norm of information security non-compliant behaviour, which produces undesirable structures of legitimisation (Andersson et al., 2022). This further highlighted a misalignment and contradiction between information security interpretive schemes in structures of signification and norms in structures of legitimisation.

5.5.3.3 *Alignment of Norms with Parent Organisation*

The misalignment between signification structures and legitimisation structures were further exemplified by the relationship between ORG₁ and its parent organisation ORG₂. While there was a sense that ORG₂ is forcing an alignment of information security through structures of domination and signification, there was an apparent misalignment of legitimisation structures with ORG₁. ORG₂ had a considerably low tolerance for information security non-compliance behaviour, with strongly enforced sanctions. ORG₁ on the other hand, had a high tolerance for non-compliance, with weakly enforced sanctions. This observation was expressed by management and security personnel, who were privy to the innerworkings of ORG₁ and ORG₂ relations pertaining to information security. For example, a security analyst explained how ORG₁'s information security initiatives were driven by ORG₂, but not enforced in accordance with the parent company's sanction level:

I think it's getting to a point where you're kind of being told what to do. And where I'm going with this is, so our parent company, ORG₂, and this is from a security point of view. We starting to get a lot of directives from them. How we should implement stuff. And what we need to implement, and how we need to implement it, so we don't really have a say as to what needs to be implemented, how it needs to be implemented, and what policies etc. No, those things are just pushed down, so it's becoming more of a top down...The access management it's...it's a really good thing, you know. But, because you need to accommodate all these various and different teams. You kind of configure this thing to accommodate all these individuals or individual teams, but it's not even, it's not optimized or configured really according to policy, to ORG₁ policy. And if we should configure it according to policy, a lot of people are going to be unhappy and not try and want to use the product.

The same view was aptly expressed by the CIO:

I think the important thing here, you have to cascade culture from the top. In other words, at organisational level and then as it cascades down into security behaviour. You will not be able to set a specific security culture if the overall higher-level culture in the organisation is of non-compliance. Okay so for instance, if you look at ORG₂, ORG₂ allows a far lower tolerance to being one of those that gets phished. They put you on disciplinary after the second time. We have people that have been caught five

times in a row and have not even had a disciplinary discussion. So it is not going to happen at the security layer. You cannot change security culture and behaviour if the overall organisational culture does not align with what you are trying to introduce at the security level.

Furthermore, most participants believed that the organisation had the authoritative power to penalise employees who violate ISPs. However, the same participants added the caveat that sanctions should be within reason. It was logical to deduce that ORG₁ employees will perceive the parent organisation's strict ISP enforcement as unreasonable and harsh. An advanced analytics and assurance specialist mooted that sanctions were acceptable, but within reason:

when it's too harsh at times, given the fact maybe it's a first occurrence, and you have a situation where there is severity, in a sense that, you get dismissals, and you get penalties that really are quite incumbent, to the point where you lose a financially in that regard. Then I think sometimes we need to have an element of, if I can say, tolerance...Penalties should be there, I understand that, but I think sometimes you know it can be severe depending on who is sanctioning it.

The structural alignment particulars of ORG₂ were not known as it is not within the scope of the case study at hand. It was evident however, that ORG₂ had a strong influence on the information security interpretive schemes at ORG₁ through domination structures. While ORG₂ was shown to exercise authoritative power over ORG₁ in the implementation of "the strictest policy" levels in the technology domain, as implied by a senior IS architect, the level of sanctions enforced in the social domain however was not aligned with this stringent level of interpretive schemes. This also implied that the level of accountability among employees were in contradiction to the expected norms, aligned with the strict level of security policies communicated in interpretive schemes.

5.5.4 Reflexive Monitoring and Change

Social actors can be self-accountable for their actions through structures of signification, domination, and legitimation (Bernardi, 2017). Human beings are knowledgeable social actors who reflexively monitor their actions and the actions of others (Giddens, 1984). Through reflexive monitoring of actions, and the rationalisation of conduct, social actors hold each other accountable to ensure human behaviour is socially acceptable (Giddens, 1979;

Bernardi, 2017). This was evidently the case when analysing the pervasive perception held of information security personnel. The analysis showed that there was a negative perception of information security personnel among skilled IT professionals. Information security personnel in this study were found to be strong motivators of ISPs that were implemented in the technology domain. The behaviour of information security personnel was reflexively monitored before and after policy implementations, to hold them professionally accountable for their actions.

Before policy implementations, it was observed that a most restrictive and a one-size-fits-all approach dominates ISP applications. For example, a technical analyst expressed:

You see the thing for me about policies is always that you have one, almost like system of policy instigators, so it would be Gartner, it would be whichever one of these consulting companies are, and most times it's a one size fits all policy that gets blanketed out or copied and pasted.

Similarly, a senior integration architect, and an advanced analytics and assurance specialist stated:

So, where there is awareness, you know, implicitly the trust is taken away, and sometimes personally, I think, like I said to you, there is one element of it, that is that willingness to understand what it is, it is just, it is easier to have a blanket thing, because it is too much effort to go and understand it.

So, you need to, in the context of let us say, for instance, in America you will get where a company deals with credit cards or a company does those transactions for them. Obviously, because it is people's money, utmost security, I mean, even the building does not have a colour or a name on it. Those type, they will go to the nth degree to make sure that they are protected and they have got all these security gates and enforcements, where at Egress, I think, yes, we are dealing with financial data, but we do not have to go to that extreme, as well. I think, whenever you do that, all you do is, you just put in additional obstacles which causes quite a big waste of time for the guys and that leads to frustration and guess what happens when people are frustrated. Then, they bypass.

A perception was therefore created that information security personnel were uninterested in understanding how ISPs in the technology domain impact an employee's norms, and their ability to achieve their goals in the social domain. That is, employees expected information security personnel to review whether the technology domain shaped their social domain adversely before implementing technology changes. This was subsequently perceived as contradictory to the organisation's cultural beliefs consistent with goal orientation and innovation orientation. As a senior integration architect further explained:

Now, what will happen with our security guys at ORG₁ as an example, they will treat everything as a system of record. So when I want to do something quick, they expect you to apply, in Azure when I am creating a logic app, the same level of security they do with SAP. Now it is not productive, because you are stifling innovation at the end of the day, because you are not applying your security policy accordingly to what is appropriate for that system and that layer that, that system is in.

Information security personnel's normative response to reported contradictions after policy implementations were also reflexively monitored. It is explained that information security personnel rarely exhibited a desire to review policy implementations for effectiveness and impact to employee norms. For example, an advanced analytics and assurance specialist explained:

But before you implement anything, just go back and review what you have done is actually a working solution...And here is again the thing. People just see it and the operational teams just see it as a tick box. Somebody has just ticked the box, so that the Board is now happy that we have got a system in place to secure it, as well.

This, in the minds of participants, contradicted the organisation's core goal-oriented cultural value of "owning-it", and being accountable. The cultural value can be considered as an institutionalised interpretive scheme and expected norm within the social domain. As a secondary data extract from a HR presentation on cultural beliefs showed "Own It! I own the results and don't blame others". The same HR communication also listed the courage to act and continuously improve as a key cultural value "Tell Me. I seek, give and act positively on feedback". This implied that skilled IT personnel in general monitored the behaviour of information security personnel, pre and post ISP implementations and felt conflicted. They monitored how ISPs were initially implemented in the technology domain. They then

experienced contradictions which impacted their performance, leading to conflict and the use of technology in a non-compliant manner. They then monitored the response of information security personnel, in light of performance impacting contradictions that were experienced.

The outcome of reflexive monitoring left the impression that information security personnel are uninterested in understanding how ISPs impact business users. The perceived behavioural response also contradicted the organisation's espoused goal-oriented cultural values of being accountable and using feedback to continuously improve. Negative interpretive schemes of information security professionals in general were therefore (re)produced in signification structures. A technical analyst and a senior integration architect confirmed:

That's a gripe that anybody in technical has, because you have a certain function to perform, so the security team will come in and say, you know what Gartner has decided that you can't have all your admin ID's now, right. So you need to use this specific application now, or this specific programme now to log in so that we can monitor your access and we can, you know ... So many times those types of things get done and it's a hindrance to a guy who's actually got ... so now he has to learn a new system firstly, he has to get used to a new way of working, and for me it's always like you have to question the benefit that actually brings to the company because you've instituted now another system, another possible point of failure, another complication... So there's different ways of doing things and not just the one way that security seems to get stuck in. I think that gets driven from, like I say going back to the Gartners and those people, and they write the rules for these things.

And honestly, sometimes, I will be quite frank with you, I think it is an ego thing with certain people. And it is not just for the ORG₁ security guys, it is broadly speaking, I hold this power over you, and therefore, I am going to flex my ego, and that is often the case as well. And that does not ultimately bode well, from a compliance point of view. If you were just reasonable and there was an element of trust, then people would work with you a lot closer.

Furthermore, evidence indicated that contradictions experienced by individuals led to feelings of frustration, and contributed to negative perceptions about information security. Table 9 and Figure 7 illustrate how themes of contradictions and reflexivity are associated with the theme of negative perceptions, which subsequently produces undesired structures of signification.

Table 9. Themes of Negative Interpretive Schemes of Information Security

Themes	Data Extract	Ref.
Contradictions create a negative perception of information security.	“When you say your security policy, for me a security policy it is like your profiles and stuff like that as well. I think that is part of it as well. So now it happens a lot where you try to complete a job, but you do not have the necessary access. But the policy says but you are not supposed to have that and then I clash with that all the time and I do not think the person that is running with it does not see the full picture.”	IPT10
Signification structures of negative perceptions are reinforced when policies impede performance.	“So that's one thing that actually hinders the project a lot and possibly delay us. So it does impede on productivity or efficiently. But again, I think it's something that's more process driven, where if the process can be a little bit faster than what it is at the moment, then we shouldn't have the problem of impeding on productivity. So if its done properly, and it's done in a way that, you know, you can remain productive or efficient, then information security policies are fine, you know.”	IPT3
Security personnel uninterested in understanding employee work practices to optimise implementation of policies (Reflexivity).	“And that is looking at it from a slightly different angle, and this is the problem that I often think that the security team at whichever level has two problems. One, they do not necessarily fully understand the context and environment they are working in, and they are not even interested in understanding it. So, they err on the side of over-regulating or over complicating policy, which I think is the problem and that influences your level of compliance at the end of the day.”	IPT16
Lack of reflexivity from information security personnel post implementations, creates the perception that they are uninterested in business needs.	“You see the thing for me about policies is always that you have one, almost like system of policy instigators, so it would be Gartner, it would be whichever one of these consulting companies are, and most times it's a one size fits all policy that gets blanketed out or copied and pasted...It's more reactionary. It's like they do it more to, companies do it more to show that they're doing something, so it's a show that say we've done this, or say we've done that, and it's more to cover their own bases as opposed to a real need to understand how people work.”	IPT13

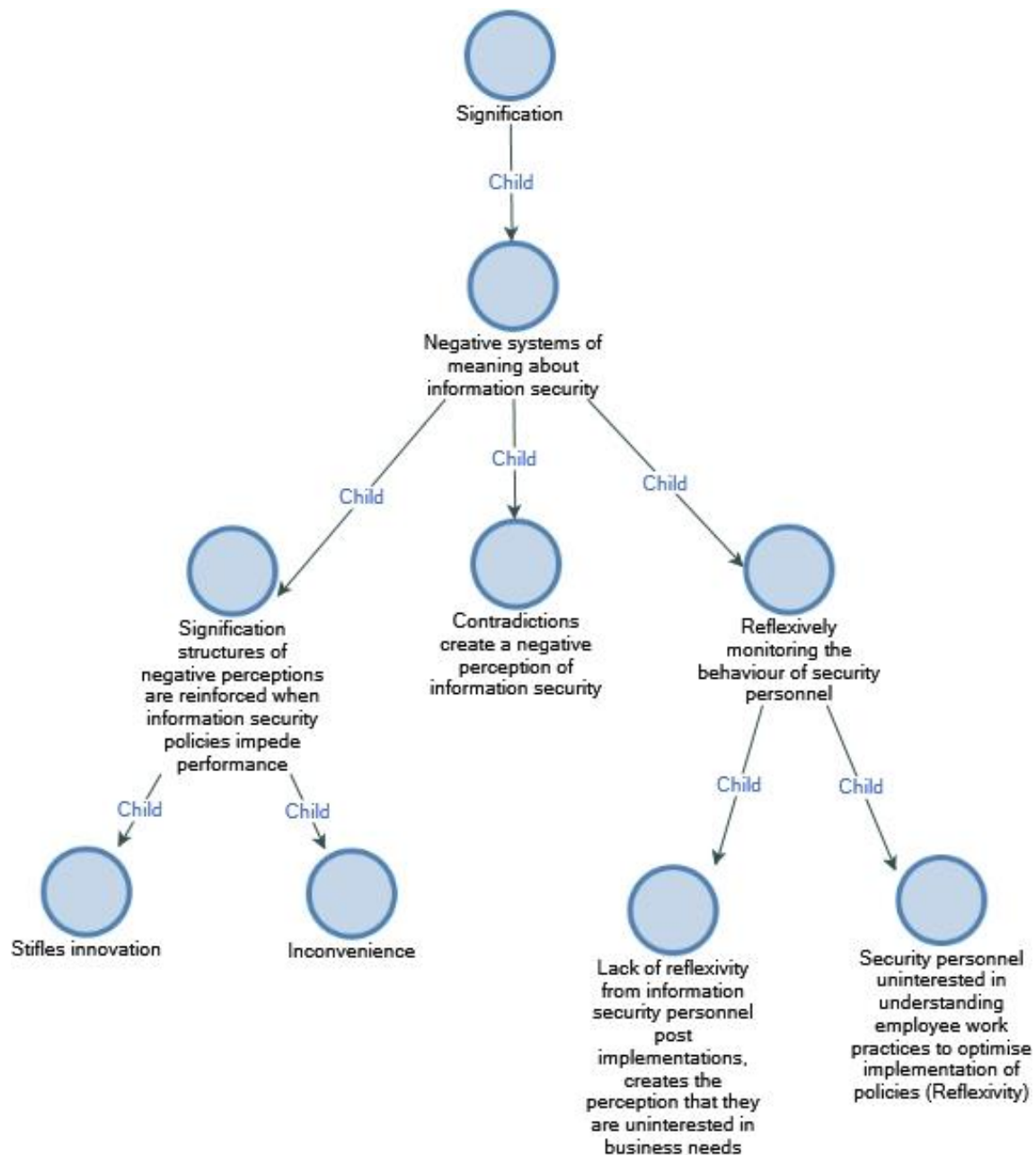


Figure 7. Themes Associated with Negative Perceptions of Information Security

The goal of this section was to describe the findings of a thematic analysis of the collected data. The findings comprised an interrogation of information security compliance behaviour, salient cultural values, cultural contradictions, conflict, and a structural analysis. Empirical evidence confirms that contradictions lead to conflict, which invariably results in information security non-compliant behaviour. Structural analysis also shows emerging contradictions in interpretive schemes, facilities, and information security norms, which lead to information security non-compliance. Furthermore, a structural examination revealed a misalignment between structures of signification, domination, and legitimation, which inhibits the achievement of the shared goal of information security compliance behaviour.

The following section will comprise a discussion and theoretical elaboration of the cultural contradictions and structural analysis results.

5.6 Summary

While training was found to increase security awareness, non-compliance to ISPs was still common among employees. This means that although training increased awareness, it failed to increase compliance behaviour. An analysis of the organisation's cultural orientation revealed goal orientation to be the salient cultural type. There was also a degree of professional trust among team members, showing evidence of a broadly professional culture. Furthermore, the organisation's information security culture was in a state of immaturity, as employees lacked information security knowledge and awareness. Top management support for information security was also in its infant stages.

This study found strong evidence of Priority Contradictions, Process Contradictions, Vision Contradictions, and Technology Contradictions, but little evidence of Role Contradictions. Employees appeared to understand their role and responsibility in information security. It was also clear that the emerging contradictions led to conflict and actual behaviour of non-compliance to ISPs.

Structurational analysis showed that non-security personnel had no knowledge of the organisation's information security goals. This led to misaligned goals of information security, as employees drew on their own information security generalisations which were antithetical to the organisation's goals. This produced misaligned structures of signification.

Analysis of structures of domination also found that information security personnel, and the parent organisation, exercised authoritative power over the ISPs to be adopted. Information security personnel subsequently drew on their professional skills to legitimise and obtain allocative resources (funding) for their information security implementations. Furthermore, the organisation was found to use cyber security training as a facility of power to communicate acceptable interpretive schemes and norms, and in turn produce desired structures of signification and legitimation. However, the training content was found to emphasise cyber security and lacked themes of information security.

An analysis of legitimation structures also showed a lack of observable sanctions for non-compliance behaviour. While the organisation implemented strict ISPs, associated sanctions for non-compliance were weakly enforced. Strict ISPs and weakly enforced sanctions subsequently produced misaligned structures of signification of legitimation, which was antecedent to non-compliance behaviour. Furthermore, while the parent organisation exercised authoritative power over the stringent interpretive schemes adopted in ISPs, it did not have the same influence on the level of sanctions enforcement in its subsidiary. This was partly due to the cultural differences between the organisations, which shaped norms in legitimation structures that were misaligned strict interpretive schemes in signification structures.

Structurational analysis also found that employees generally experienced ISPs to impede their ability to perform their professional tasks. Employees would then monitor the response of security personnel to these impediments, expecting a compromise. When efforts of compromise were not apparent, a perception that information security personnel were uninterested in the business impact of ISPs were formed in the minds of employees. This produced and reproduced undesirable interpretive schemes which informed, and was informed by, negative structures of signification.

6 Discussion and Theoretical Elaboration

This section endeavours to discuss and synthesize the findings of the previous section. Having answered the secondary research objectives by establishing the level of compliance behaviour, and identifying the contradictions that emerge, this section will seek to conduct a theoretical elaboration on how contradictions influence compliance behaviour. While relying on Walsham's (2002) adaptation for a structural analysis on cultural contradictions, this study employed Bernardi's (2017) use of Structuration Theory in understanding the role of cultural contradictions in information security compliance behaviour.

6.1 Cultural Contradictions and Compliance Behaviour

Cultural analysis showed that organisations that are goal-oriented, which is situated on the control and external axis of the CVF continuum (Faerman & Quinn, 1985), emphasise goal achievement as an integral part of the overall employee performance appraisal process. Although goal-setting could vary per subculture or group, all employee performances within goal-oriented cultures are generally evaluated based on goal achievement. In addition, accountability among employees is a key characteristic of goal-oriented cultures (Cameron & Quinn, 2011).

Evidently, Cameron and Quinn's (2011) generalisation is validated, that cultures which encourage continuous improvement, and creating new ways of working, tend to be innovative in their orientation. Moreover, professional cultures clearly have a strong influence on the information security compliance behaviour of employees (Kolkowska, 2011). Professional cultures are founded on distinct characteristics which are unique to an individual's profession (Ramachandran, Rao, Goles, & Dhillon, 2013). Respective teams within an organisation could therefore have varying degrees of goal orientation, innovation orientation, and professional culture orientation. This confirms a dynamic view of culture within research (Straub et al., 2002; Karahanna et al., 2005; Leidner, 2010), where a cultural orientation is not uniformly shared by all members within the group.

Furthermore, this study confirmed the information security relevance of cultural contradictions in the forms of Priority Contradictions, Process Contradictions, Technology Contradictions, and Vision Contradictions, as proposed by Geeling et al. (2017). All relevant cultural contradictions were found to emerge in the process of employee compliance

behaviour towards ISPs, as outlined in Table 10. Priority Contradictions can occur when there is a misalignment between value systems which inform how individuals and groups prioritise aspects of information security. Although employees mostly agreed that information security is a priority, they however questioned its criticality compared to their own productivity, which resulted in conflicting priorities. This is supported by prior research, which postulates that employees will often experience value conflict when a prioritisation of security values underpinning ISPs conflicts with their own professional values (Hedström, et al., 2011). Given the prominence of professional cultures within organisations (Karahanna et al., 2005), it could be argued that conflict between employee professional values and embedded information security values are imminent (Ramachandran, et al., 2013). Kirlappos et al. (2013) also showed that employees will decide not to comply with ISPs if they are deemed to conflict with their professional values and productivity activities.

Table 10. Cultural Contradictions Implicated in Compliance Behaviour

Cultural Contradictions	Definition	Implicated in Compliance Behaviour
Priority Contradictions	Occur when the value systems which inform how employees and groups prioritise their tasks are misaligned (Geeling, et al., 2020).	The professional values shared by employees contradict the values embedded in ISPs. Employees prioritise their professional values over ISPs.
Process Contradictions	Occur when differences in work practices emerge between groups because of divergent values which inform those practices (Geeling, et al., 2020).	The values embedded in ISPs contradict the daily tasks of employees. Employees choose their professional tasks over compliance to ISPs.
Technology Contradictions	Arise from differences in assumptions and beliefs about technology between groups and its embedded functionality (Geeling, et al., 2020).	Security values embedded in technology contradict the professional values of employees. Employees choose to bypass ISPs when they conflicts with business tasks.

Vision Contradictions	Arise as a result of misaligned goals between stakeholders who are engaging with technology (Geeling, et al., 2020).	Information security goals embedded in technology contradict the professional goals of employees. ISPs are circumvented to achieve professional goals.
-----------------------	--	--

Process contradictions were also implicated in the process of information security compliance behaviour, which generally occur when differences in work practices emerge between groups because of divergent values which inform those practices (Geeling, et al., 2020). Process contradictions in information security will occur when information security processes impede the daily tasks of employees. This confirmed prior studies which found that employees will perceive information security compliance as “not worth it” (Kirlappos, et al., 2013, p. 7) when ISPs hinder their business processes. Employees generally consider information security values underpinning policies equally important as their own professional values. However, when asked to choose between the two, they will invariably choose their professional tasks over compliance to security policies (Kolkowska & De Decker, 2012; Chang & Seow, 2014). Contradictions and conflict commonly occur because ISPs will likely require employees to take extra steps in their daily work processes, which hampers their efficiency and productivity (Xu & Guo, 2019). Previous research have shown that ISPs are often incompatible with work processes and practices (Adams & Sasse, 1999; Kirlappos, Beautelement, & Sasse, 2013).

Technology contradictions were also found to be implicated and of relevance to information security. Technology contradictions, according to Geeling, et al. (2020), can arise from differences in assumptions and beliefs about technology and its embedded functionality. The information security values embedded within technology were found to conflict with the daily business practices of employees. This corroborated previous studies which found that ISP impediments to work practices affect compliance behaviour negatively (Hwang & Oona, 2018). Researchers have therefore recommended that organisations should focus their efforts on ensuring that information security mechanisms and technology are effectively meshed with the business needs and tasks of employees (Kirlappos, et al., 2013).

Effective information security management necessitates an alignment of information security goals between the organisation’s management and information security personnel

(Ramachandran et al., 2013). However, of equal importance is the alignment of information security goals between non-information security personnel and the organisation's information security goals. A lack of information security goal alignment between the organisation and its employees, according to Guo et al. (2011), leads to goal contradictions and affects information security compliance behaviour negatively. Previous studies have shown that employees are likely to prioritise their own goals over information security goals when experiencing contradictions, especially when they have limited resources, time and energy (Van Niekerk & Von Solms, 2010; Karlsson, Karlsson, & Åström, 2017; Xu & Guo, 2019). Moreover, the foregoing of information security goals in the interest of business goals is found to be especially apparent where job performance and goal orientation are key cultural values (Guo, et al., 2011). This finding was supported by this study, as employees within goal-oriented cultures are inclined to abdicate responsibilities associated with information security goals, and focus on their job performance and professional goal achievement instead. Thus, researchers have cautioned against information security goals which contradict employee performance indicators, and recommend security goals be included in employee performance evaluations instead (Ruighaver, Maynard, & Chang, 2007; Hwang & Oona, 2018).

6.2 Enacted Structures of Information Security Compliance Behaviour

This section sought to report on the structurational analysis results and advance theoretical elaborations on the findings. The discussion entails a delineation of the focal findings that are pertinent to answering the research question at hand, which are presented as enacted structures in the process of compliance behaviour. The structural analysis results confirmed the concepts of contradictions in structural principles that can lead to conflict, which is the actual struggle between social actors and groups (Giddens, 1984). This study showed that various forms of cultural contradictions can emerge within organisations, which can lead to conflict and non-compliance outcomes. According to Walsham (2002), although culture is rarely uniform, social structures often resemble a sufficient degree of systemness to be regarded as being shared by a group or culture. Researchers also argue that the material features of technology typically reflect an organisation's embedded values, interpretive schemes, and norms (Orlikowski, 1992; Walsham, 2002). Similarly, information security, which is at the centre of IS (Lowry, et al., 2017), reflects the underlying security values, interpretive schemes and expected normative behaviour of the organisation (Hedström, et al.,

2011; Kolkowska & Dhillon, 2013; Cram, et al, 2017; Paananen, Lapke, & Siponen, 2020). Organisations can therefore instil their information security values and interpretive schemes within IS through ISPs and features, which are organisational artefacts that aid in the formation of a security culture (Lowry, et al., 2017; Da Veiga, et al., 2020; Solomon & Brown, 2021). This, according to Bernardi (2017), is how designers and implementers in the social domain shape the information security features and policies in the technology domain.

Following is a discussion of key findings on how:

- (1) Security training content which is misaligned with information security goals, produces signification and legitimation structures which reinforces non-compliance to ISPs.
- (2) Employee information security goals in the social domain, which are misaligned with those embedded in the technology domain, reproduce an understanding that information security is unimportant, which forms the grounds for ISP circumvention.
- (3) Misalignment between interpretive schemes underpinning signification structures, and weakly enforced sanctions propagated in legitimation structures, influence the ISP compliance behaviour of employees.
- (4) Structures of domination typically enacted within multinationals produce contradictory signification and legitimation structures, which adversely affect the diffusion of information security professional responsibilities, and the subsequent compliance behaviour of employees.

6.2.1 Information Security Training and Compliance Behaviour

This section aims- to elaborate on the theme of training and education, and its implications on signification, domination, and legitimation structures, as well as the consequences on compliance behaviour. Central to the conceptualisation of the duality of structure is the knowledgeability of human actors (Orlikowski, 1992). In accordance with Giddens's (1984) emphasis on the knowledgeability of social actors, knowledge of the organisation's interpretive schemes (systems of meaning) is necessary for individuals to act in a socially acceptable manner (Sewell, 1992). Extant literature also shows that knowledge of ISPs, and associated risks, precedes an information security culture that exhibits desirable compliance behaviour (Van Niekerk & Von Solms, 2010; Da Veiga & Martins, 2015). The communication of interpretive schemes, in the form of appropriated information security

awareness training, becomes important to produce favourable structures of signification (Parsons et al., 2014; Arhin & Wiredu, 2018).

Although extant literature shows a lack of consensus on the dimensions which constitute an information security culture, researchers agree that information security knowledge and awareness is a definitive dimension (AlHogail, 2015; Nasir, et al., 2019; Da Veiga, et al., 2020). Through particularised awareness training, organisations can increase employee knowledge of ISPs embedded in the technology domain, and thereby accelerate the instillation of an information security culture with desired interpretive schemes (Ifinedo, 2012). An intended consequence of an effective training programme is to shape the way employees use technology, in a manner that conforms to ISPs (Haeussinger & Kranz, 2017). This shaping is ultimately intended to produce signification and legitimation structures in the minds of employees, which reflects a coherent understanding of ISPs that is aligned with compliance behaviour (Bernardi, 2017; Arhin & Wiredu, 2018). This was evinced by this study's findings, which showed that cyber security training had a positive influence on employee compliance and interpretation of cyber security policies. This also corroborates extant literature which posits that security training can serve to increase stocks of knowledge about security policies among employees (Ifinedo, 2012; Parsons, et al., 2014). It is therefore widely accepted that an effective security training programme is necessary to improve security risk awareness and compliance behaviour (Safa, et al., 2016), and to instill an information security culture (Da Veiga, et al., 2020; Solomon & Brown, 2021). Awareness training is also significant in realising effective ISPs (Soomro, Shah, & Ahmed, 2016). Information security awareness is therefore a strong predictor for information security compliance behaviour (Haeussinger & Kranz, 2017). Furthermore, Bulgurcu et al. (2010) show that information security awareness training can mitigate the negative perception or interpretation that ISPs impede performance, which is confirmed by this study.

Organisations can therefore exercise power by using training programmes as an authoritative resource to facilitate the communication of intended information security rules, consisting of interpretive schemes, and expected normative conduct. However, as Giddens (1984) argues, actions are usually accompanied by a mixture of intended and unintended consequences, which indirectly affect the wider institutionalised social system of agents. Unintended consequences in structurational terms are the unexpected possibilities resulting from the actions of actors (Giddens, 1979). The implementation of IS applications in general can have

new implications on the larger social system which were unconceived at the time of original design (Lyytinen & Ngwenyama, 1992). Figure 8 illustrates the unintended consequences of an organisation's cyber security training and awareness programme, which is ineffective in producing information security compliance behaviour outcomes. The findings show that the content of an organisation's training programme is a strong determinant of its effectiveness, and employee non-compliance to ISPs as an unintended consequence. When training programmes exclusively communicate cyber security, while omitting information security in general, interpretive schemes are produced that are misaligned with the ISPs that are implemented. This finding is consistent with the research distinction between cyber and information security. Cyber security involves the protection of information in cyberspace, whereas information security involves the protection of information everywhere (Reid & Van Niekerk, 2014; von Solms & von Solms, 2018).

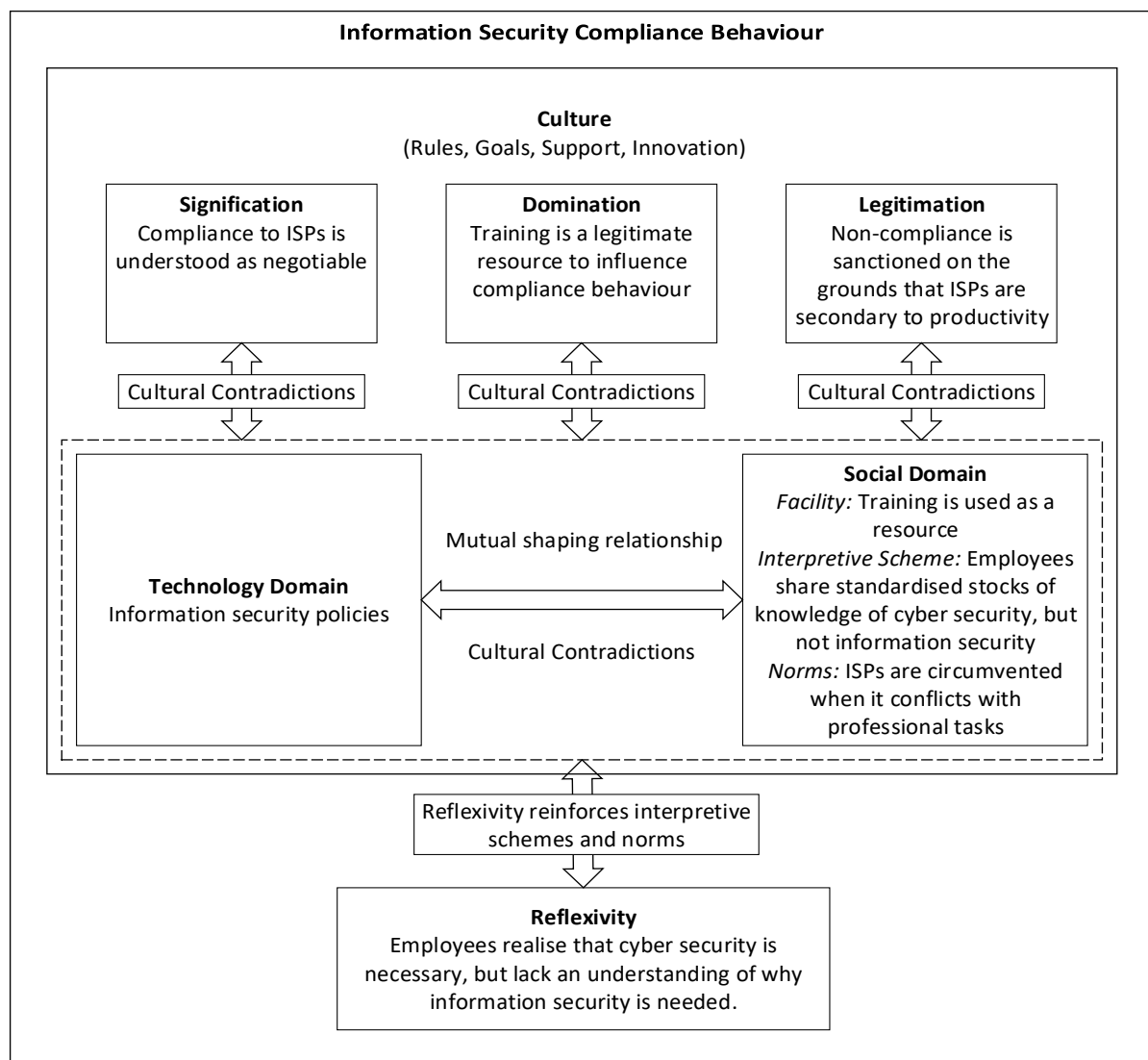


Figure 8. Information Security Training and Compliance Behaviour

While employee understanding of cyber security risks was enhanced with cyber security training, their understanding of information security risks remained unchanged. That is, although employees could share stocks of knowledge about cyber security, they lacked shared interpretive schemes to inform their interpretation of ISPs in a manner that is aligned with their organisation's understanding. This defeats a primary objective of information security training, which is to augment the interpretive schemes of employees with knowledge of information security risks and associated policies (Parsons, et al., 2014; Safa, et al., 2016).

In addition, Halperin and Backhouse (2007), in highlighting the richness of interpretive schemes, argue that the modality encompasses both knowledge of technology and the self-efficacy of employees. Self-efficacy refers to an individual's conviction that they possess the capability and knowledge to adhere to ISPs (Bandura, 1977; Safa, et al., 2015; Cram, D'Arcy, & Proudfoot, 2019). Self-efficacy is also found to be a strong predictor of information security compliance behaviour, which can be improved with training and education (Siponen, et al., 2014). Training programmes which focuses exclusively on cyber security will therefore be ineffective in enhancing employee knowledge of information security interpretive schemes and, by implication, fail to strengthen employee self-efficacy and confidence in their ability to comply with ISPs.

When the communication of interpretive schemes which are misaligned with ISPs ensues, contradictions arise between the social domain and the technology domain. This implies that the interpretive schemes held by employees will contradict those embedded in ISPs.

Differences in frames of reference held by individuals or groups can lead to meaning contradictions (Ravishankar, 2015). The contradictions that emerged were expressed as forms of priority, process, technology, and vision contradictions, which are generally shared by employees. Shared contradictions, according to Walsham (2002), indicate a degree of systemness and infer cultural contradictions. Geeling and Brown (2017) show how cultural contradictions arise because of divergent values, beliefs and norms held by individuals and groups. While ISPs can implicitly incorporate the interpretive schemes and norms held by the organisation, the observable norms of employees however reflected a common understanding that compliance to ISPs were deemed secondary to their own priorities, vision, and daily practices. When information security interpretive schemes and norms embodied within the technology domain, contradict the observed normative behaviour and interpretive schemes held by employees, the unintended consequence of non-compliance to ISPs is realised. This

finding confirmed extant literature that contradictions usually lead to conflict, and a subsequent circumventing of ISPs (Karlsson, et al., 2017; Li, Pan, & Zhang, 2020; Cram, Proudfoot, & D'Arcy, 2021). However, an empirical examination of social structures enacted in the process of training and compliance behaviour has not been conducted, which is a novel contribution of this study.

The findings showed that where ISPs conflict with employee professional tasks, and where cyber security training instead of broader information security training is implemented, the unintended consequence of employee non-compliance to ISPs ensues. This confirms the assertion that employees are likely to develop workarounds to IS policies which are deemed to limit their ability to complete work tasks (Davison & Ou, 2018). Interactions in the social domain result in the production of signification structures where compliance to ISPs is understood to be negotiable, and legitimation structures where non-compliance is warranted because it is deemed secondary to productivity. Although the intention of training programmes is to influence compliance behaviour positively, the unintended consequence of misaligned security training is the production of signification and legitimation structures which explicates both the reason and justification for non-compliant behaviour.

This highlights the need to evaluate the context and content of the material communicated in information security training programmes. Parsons et al. (2014) show that generic training is ineffective and proposed contextualised content instead, that improves employee knowledge of ISPs. Researchers have consistently shown that compliance to an ISP necessitates knowledge and understanding of the given policy, providing sufficient interpretive schemas for employees to draw upon in compliance behaviour (Chen, et al., 2015; McCormac, et al., 2017; Hwang, Wakefield, Kim, & Kim, 2021).

In addition, knowledge of ISPs influences compliance behaviour, which subsequently contributes to the formation of a desired information security culture (Reid & Van Niekerk, 2014; Flores & Ekstedt, 2016). It is worth noting the difference between an information security culture and a cyber security culture in literature. While information security is contextualised to the cultivation of a culture within the confines of an organisation, cyber security culture has a broader societal context in cyberspace (Reid & Van Niekerk, 2014). Information security culture is commonly defined as the values, attitudes, and assumptions towards information security, which are shared by members of an organisation (Da Veiga & Eloff, 2010). Cyber security culture on the other hand, can be defined as the values, attitudes,

and assumptions towards information protection in cyber space, which are shared by a group (Da Veiga, 2016). While the cyber security training increases cyber awareness, and advances a cyber security culture, it leaves a deficiency in interpretive schemes pertaining to ISPs and fails to contribute to an information security culture. Research corroborates this finding, which shows that ineffective information security training results in insufficient ISP knowledge (Albrechtsen & Hovden, 2009). Thus, it fails to increase employee knowledge and understanding of the organisation's ISPs, which is a key contributor to non-compliant behaviour (Hwang, et al., 2017). The evidence therefore confirms that ineffective information security training programmes can lead to structures of signification and legitimation which contradict the organisation's security goals, and ultimately provides the rationalisation and justification for non-compliant behaviour.

6.2.2 Information Security Goals and Compliance Behaviour

This section expounds on the structures enacted in the process of information security goal achievement, and its consequences on compliance behaviour. Evidence in this study showed that goal-oriented organisations typically evaluate employee performance against goal achievement, while also emphasising accountability as a cultural value, which validates key characteristics of the CVF (Van Muijen, et al., 1999; Cameron & Quinn, 2011). In addition, a confirmatory finding of the CVF is employee goals that are filtered down from top management, with the intention of maintaining alignment with the organisation's strategic goals, is a key characteristic of goal orientation (Faerman & Quinn, 1985).

Further to strategic goal alignment, information security goals should ideally be incorporated and aligned with the organisation's goals (Ramachandran, et al., 2013), which implies they share the same structures of signification. This study showed strong evidence that goal alignment between information security initiatives and the overall organisational strategy has positive implications on ISP implementations. ISPs should ideally reflect the official beliefs and goals of the organisation (Paananen, et al., 2020). As Karlsson et al. (2017) argued, ISPs are communicative objects in and of themselves, the content of which should be high in quality. As illustrated in Figure 9, goal alignment evidently strengthens a security team's ability to obtain monetary resources, allowing them to implement information security initiatives to achieve their goals. Security professionals also use their skills and that of industry vendors to support their motivation for funding. Skills as an authoritative resource, and funding as an allocative resource, is necessary for ISP development and implementation

(Andersson, et al., 2022). Thus, structures of domination are produced which reflect the legitimate use of funding and professional skills as resources to achieve information security goals.

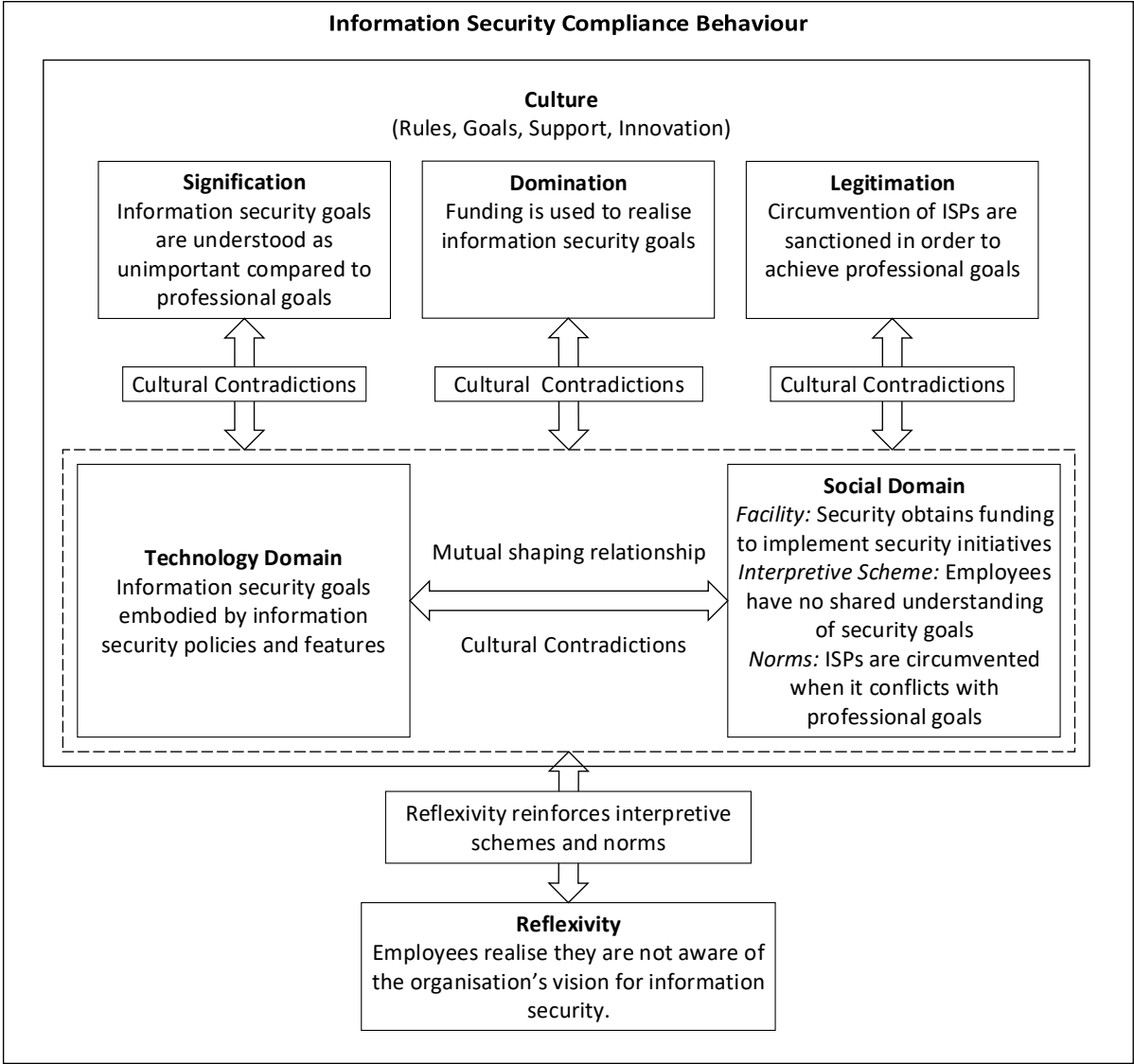


Figure 9. Information Security Goals and Compliance Behaviour

However, structurational analysis findings showed that where employees, through the process of reflexive monitoring, acknowledge that they were unaware of the organisation’s information security goals, it usually indicates a misalignment between the information security goals of the organisation, and that of employees. Thus, employees drew on interpretive schemes in interaction which were misaligned with the organisation’s security goals. This partly occurs when the communication of ISPs and their associated goals to employees are largely absent. Research emphasises the importance of the communication of ISPs that are congruent with the organisation’s overall strategy and standards (Karlsson, et

al., 2017). This highlights the notion that ISPs comprise the organisation's security goals, the communication of which relays the organisation's security values and increases the likelihood of creating a security compliant culture (Chen, et al., 2015; Lowry, et al., 2017).

The findings showed that by not communicating ISPs, employees had no knowledge or understanding of their organisation's security goals and values. Researchers have shown that where competence is low, employees will rationalise their behaviour based on their limited knowledge of information security goals (Simon, 2000; Hwang, et al., 2017). The reflexive monitoring of action is ultimately dependent on the competence, self-efficacy, and knowledge of agents (Giddens, 1984; Cram, et al., 2019). This finding confirms research which posits that insufficient knowledge of information security goals leads to a lack of understanding of security risks (McCormac, et al., 2017). Researchers therefore argued that ISPs, which inherently communicate security goals, should be visibly advertised, if employees are expected to conduct themselves in a manner that is consistent with the organisation's vision for security (Hwang, et al., 2017).

With no clear shared understanding of the organisation's vision for information security, employees tend to draw from interpretive schemes in the social domain which are misaligned with the technology domain, leading to experiences of goal contradictions. This study showed that goal contradictions occur when information security goals contradict and impede individual performance goals, which corroborates extant literature (Hedström, et al., 2011; Hwang, et al., 2017; Karlsson, et al., 2017). Experiences of goal contradictions, which are widely shared by all employees, can be deduced to be a cultural norm shared by group members (Walsham, 2002). The goal contradictions experienced by employees subsequently shaped how employees interpret ISPs and use technology. Research shows that employees will invariably prioritise their own goals when experiencing goal contradictions, which can lead to conflict and non-compliant behaviour (Hedström, et al., 2011; Karlsson, et al., 2017; Hwang & Oona, 2018; Xu & Guo, 2019; Karjalainen, Siponen, & Sarker, 2020). This sentiment is validated by this study's findings, which showed that goal contradictions will lead to conflict with professional goals, resulting in norms of ISP circumvention. The finding also supports the assertion that an individual's daily practices are predominantly influenced by their professional culture (Karahanna et al, 2005). While the goal of information security is to protect the organisation's informational assets, the goal of non-security personnel is to support the business (Van Niekerk & Von Solms, 2010). This disparity in goals between the

organisation's security vision and that of individual group members has an impact on information security compliance behaviour (Guo et al., 2011). Employees are likely to prioritise their professional goals where goal conflict with ISPs occurs (Karlsson, et al., 2017).

The emerging goal contradictions between the social and technical domain, ultimately results in the production of signification structures which reflect an understanding that security goals are of less importance compared to professional goals. In addition, this reasoning also has implications on structures of legitimation, as employees will typically justify the circumvention of ISPs to achieve professional goals, which ultimately propagates as acceptable professional practices within the team (Orlikowski, 1992). An unintended consequence of not communicating the organisation's information security goals to employees, is therefore the production of legitimation structures which provide normative grounds of justification for non-compliant behaviour in the minds of employees. This structural property contradicts the organisation's intended vision for information security, as embodied within its technology domain.

Furthermore, although findings showed little evidence of Role Contradictions, it is however argued that Role Contradictions can emerge with a lack of knowledge of ISPs (Hwang & Oona, 2018). That is, employees can experience a degree of confusion and role ambiguity when they lack a clear understanding of a given ISP (Chen, et al., 2021). It is therefore clear that goal contradictions lead to conflict, and the production of signification and legitimation structures which forms the basis and justification for non-compliance in the minds of employees.

The following section advances theoretical considerations on how power relations with a parent organisation can affect employee information security compliance behaviour.

6.2.3 Information Security Sanctions and Compliance Behaviour

The aim of this section is to elaborate on the social structures enacted in the process of information security compliance behaviour within a multinational organisation. This study's findings showed that cultural differences within a multinational have implications on information security compliance behaviour. Evidence showed that parent organisations generally have authoritative power (Giddens, 1979) to influence the information security interpretive schemes embedded in their subsidiary's technology domain. The intention of the

facility is to align ISPs and interpretive schemes with the parent organisation, thereby limiting the interpretive flexibility of technology for all employees (Bernardi, 2017). Interpretive flexibility is the extent to which the material features of technology limits human involvement in its social and material constitution during design and use (Orlikowski, 1992). The interpretive flexibility is therefore intended to shape the interpretation and use of technology among employees in a manner that aligns with ISP compliance.

The enacted facility subsequently produces structures of domination in a subsidiary which legitimises its parent organisation's authority to align security initiatives. The practice of parent organisations drawing upon authority as a facility of power to mobilise and align ISPs, is common among multinational organisations (Yayla & Lei, 2018). This notion was confirmed by this study's findings, which also showed a tendency in management to qualify the facility of power on the basis that information security risks are the same everywhere, regardless of context. This is consistent with the traditional view associated with industry standards and vendors (ISO, 2014; Gartner, 2018), which findings showed has an influence on an organisation's information security initiatives in the technology domain. A similar influence is found by Andersson (2022), who shows that industry experts often exert pressure on an organisation's interpretive schemes for their benefit. The view that security risks are the same everywhere is also supported by the generalisation that the overall objective of information security is to uphold the confidentiality, integrity, and availability of information assets (Chang & Lin, 2007; Reid & Van Niekerk, 2014). However, analysis results suggested that the manner of achieving the overall objective of information security in a multinational organisation might differ by organisational and national context, as substantiated in literature (Leidner & Kayworth, 2006; Da Veiga & Martins, 2017; Paananen, et al., 2020).

As Figure 10 illustrates, employees reflexively monitor their own compliance behaviour and the behaviour of others around them within the social domain. This is in line with security research, which shows that employees generally monitor and follow the norms of their peers (D'Arcy, Hovav, & Galletta, 2009; Hwang, et al., 2017). In addition, employees also monitor imposed sanctions and the unintended consequences of their non-compliant behaviour and that of others within the social domain (Tsohou, et al., 2015). According to this study's findings, there is a correlation between low levels of compliance to ISPs, and low levels of imposed sanctions for policy violations. That is partly because employees reflexively monitor their own actions within the social domain, and the actions of their peers where sanctions are

weakly imposed, and observe no consequences for non-compliant behaviour (Bernardi, 2017). Employees in turn, through the process of reflexive monitoring, draw on interpretive schemes within the social domain, which communicates that professional responsibilities ought to be prioritised over ISP compliance. This is an unintended consequence as it tends to contradict the intentions of a parent organisation's interpretive schemes embedded within the technology domain.

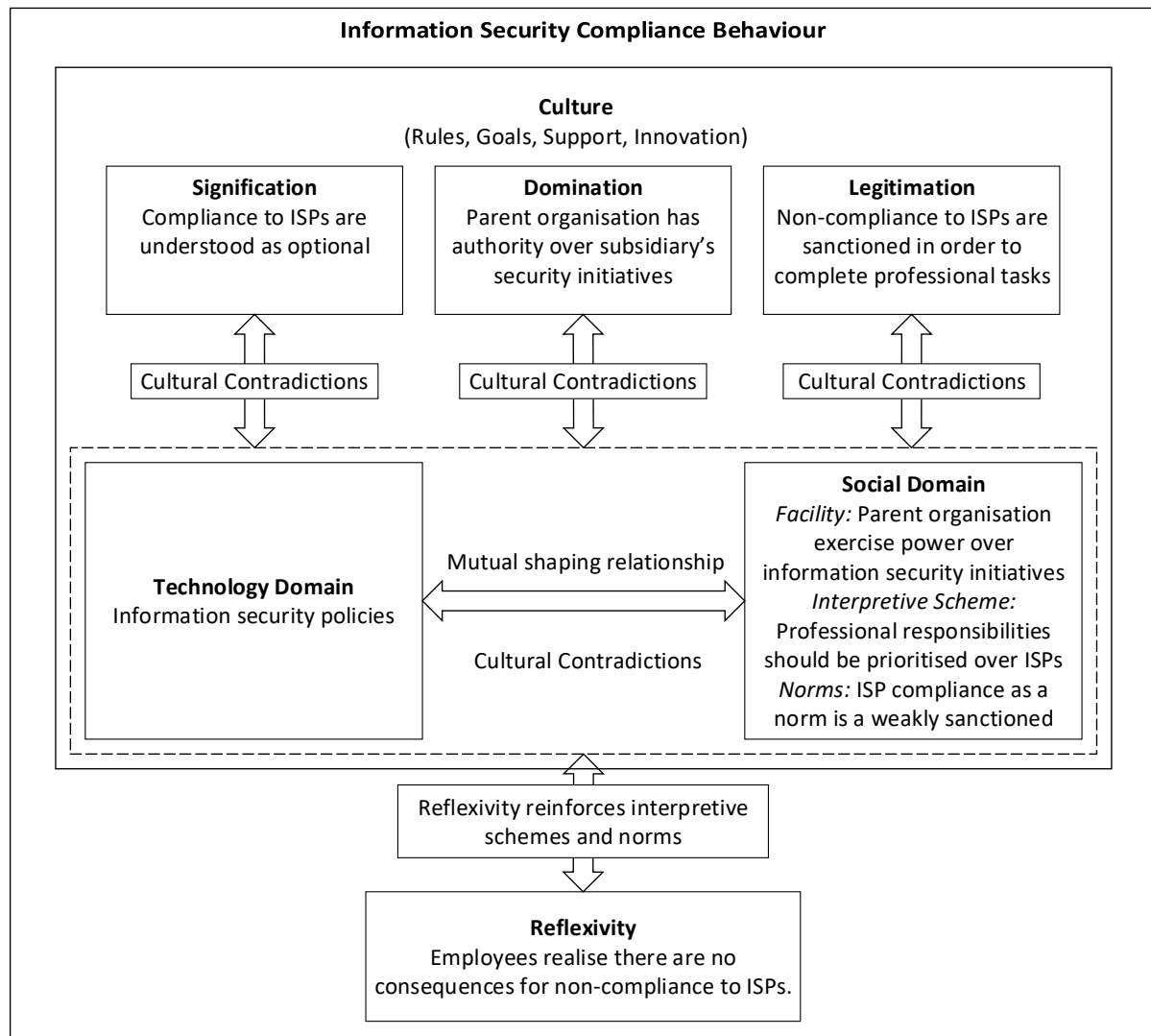


Figure 10. Information Security Sanctions and Compliance Behaviour

Structures of signification are subsequently produced in the minds of employees which reflect an understanding that compliance to ISPs are optional. It could be argued that the rationale that ISPs are optional may lead to weak intentions to comply. Intentions capture the measure of strength in motivation to comply with ISPs (Ajzen, 1991). Weak intentions to comply are found to mediate compliance behaviour negatively when experiences of contradictions occur (Karlsson, et al., 2017). Professional responsibilities are therefore given a higher priority

within the social domain over ISPs in the technology domain. Drawing on interpretive schemes in the social domain which contradict embedded interpretive schemes within the technology domain, results in experiences of conflict as employees interact with technology.

Furthermore, signification structures which rationalises ISP compliance as optional, and thereby set a higher priority on productivity, also have implications on structures of legitimation and modalities of norms, especially in experiences of contradictions.

Contradictions in this study can be conceptualised as cultural values due to their degree of systemness (Walsham, 2002), as the experience was shared by all participants. Findings showed strong evidence of Priority Contradictions and Process Contradictions leading to conflict, which is expressed as hindering productivity. This confirms extant literature which argues that ISPs in general are perceived to hinder productivity (Bulgurcu, Cavusoglu, & Benbasat, 2010; Van Niekerk & Von Solms, 2010). Drawing on interpretive schemes which prioritise productivity over compliance, and by observing no consequences for non-compliance in the social domain, employees disregard ISPs when experiencing conflict. Legitimation structures are subsequently produced where ISP circumvention is sanctioned in order to complete professional tasks. The rationale which explicates this memory trace in the minds of employees is the associated signification structure, that ISPs are understood to be optional while professional tasks are obligatory. The contradiction and misalignment in structures, Bernardi (2017) argues, hinders an organisation from achieving a common goal, which in this study is compliance to ISPs.

In the interest of further interrogation, it is pertinent to evaluate the contextual differences and complexities within multinational organisations, which could potentially contribute to contradictions and structural misalignment (Yayla & Lei, 2018). Results showed that organisational tolerance for employee non-compliance to ISPs can differ within a multinational, which influences ISP compliance behaviour. A subsidiary with high tolerance for non-compliance was shown to exhibit reasonably average levels of compliance to ISPs, with no indication of applied sanctions and consequence management. A parent organisation with reasonably lower tolerance on the other hand, exhibited higher levels of compliance behaviour to ISPs, with imminent sanctions against first-time policy violations. This implied that an organisation's strict approach to ISPs should be in accordance with strongly enforced sanctions, an alignment which is necessary for effective ISP development (Andersson et al., 2022). In contrast however, when a subsidiary with weakly enforced sanctions is obliged to

adopt the same strict policies as part of security alignment within a multinational, misaligned structures of signification and legitimation are formed. Research shows that weakly enforced sanctions and lack of consequences contribute to producing undesirable structures of legitimation, where non-compliant behaviour is a norm (Andersson et al., 2022).

Furthermore, the alignment of sanctions with interpretive schemes is necessary if an organisation wants all employees to achieve a common goal, which is compliance to ISPs (Tsohou, et al., 2015; Bernardi, 2017). The misalignment of structures of signification and structures of legitimation are therefore a contributing factor to the undesirable levels of compliance within a multinational.

In addition, there are cultural aspects to consider in the implementation of ISPs at a multinational subsidiary (Karahanna, et al., 2005; Gelfand, Erez, & Aycan, 2006).

Researchers recommend that distinct national, organisational, and subcultures should be examined for effective information security management (Faily & Fléchais, 2010; Dhillon, et al., 2016). This study demonstrates how distinct cultural differences within a multinational influence the compliance behaviour of employees. Parastatal organisations are generally hierarchical with a strong emphasis on the enforcement of rules, while a goal-oriented organisation emphasises goal achievement and innovation (Van Muijen, et al., 1999; Cameron & Quinn, 2011). These contrasting cultural orientations have ramifications on employee compliance behaviour and should be accounted for in ISP implementations.

Further, employees within a hierarchical organisational culture are also more inclined to follow strict ISPs than in a goal orientated culture (Da Veiga & Martins, 2017). Tight cultures, such as the parent organisation, usually have strong sanctions with low tolerance for deviations from societal norms (Gelfand, et al., 2006). Loose cultures on the other hand, such as the case study at hand, have less formality in norms, and have a higher tolerance for deviations. Moreover, research shows that sheer distance between organisations has the potential to contribute to cultural challenges, which is evinced by this study's findings (Connaughton & Shuffler, 2007). The clear cultural differences within a multinational should therefore be accounted for in ISP development and implementation.

Moreover, it is often the intention of top management to create one culture (Zaidman, Schwartz, & Te'eni, 2008), which is a motivating factor for aligning information security initiatives within a multinational. Yayla and Lei (2018) pointed out that parent organisations often use policies to legitimise their own practices, and thereby create new values or

normative requirements in their affiliates. While the sharing of resources and other assets in a multinational organisation might be advantageous, compelling subsidiary employees to adhere to ISP requirements of the parent organisation can be a challenge (Yayla & Lei, 2018). Subsidiary organisational members are thereby forced to consider the contradictory information security values of their parent organisation, which is evident in this study. Siponen and Willison (2009) therefore argued that the scope of ISPs should be company-specific, as opposed to generic and universally applied.

The cultural differences subsequently lead to a decrease in ISP acceptance, which also correlates with the degree of institutional distance in a multinational organisation (Yayla & Lei, 2018). Researchers contend that institutional distance provides an alternative account for employee behaviour within multinational organisations (Xu & Shenkar, 2002). Institutional distance refers to the degree of similarity or difference between a parent and subsidiary organisation (Kostova & Zaheer, 1999). The greater the institutional distance within a multinational organisation, the greater the challenge for the parent organisation to legitimise its ISPs in its subsidiary. The institutional distance in this study was bound to be great, where the multinational organisation was located in Africa and Asia respectively. This, according to Yayla and Lei (2018), ultimately has a negative effect on the diffusion of ISPs in subsidiaries.

In furthering a structural analysis in this study, it is pertinent to be mindful of the interconnectedness of rules relating to meaning constitution, and rules relating to sanctioning normative conduct. All social practices are situated in the intersections between interpretive schemes and norms (Giddens, 1979). Additionally, the communication of interpretive schemes in interaction has normative elements to it. For example, one must give an account as well as being accountable for one's conduct. Sanctioning conduct therefore becomes important, according to Giddens (1984), as it regulates the normative behaviour of actors to what is deemed acceptable conduct as communicated in rules relating to interpretive schemes.

While some have critiqued the overreliance on sanctions as a form of deterrence (Hedström, Kolkowska, Karlsson, & Allen, 2011; Ifinedo, 2014; Cram et al., 2017), it is however a necessary aspect of ISP enforcement (Cheng et al., 2013; Cram et al., 2019). Moreover, the effectiveness of ISPs is partly dependent on the level of sanctions and the consistent enforcement thereof (Knapp, Marshall, Rainer, & Ford, 2006; Cram et al., 2017). The strength of information security legitimisation structures is determined by the level of sanctions

that are enforced (Andersson, et al., 2022). Halperin and Backhouse (2007) made the distinction between varying levels of sanctions, arguing that norms can be strongly or weakly enforced and understood. Using these levels of sanctions to analyse the degree of participation in a structure, Andersson et al. (2022) showed how weakly sanctioned norms explain the behaviour of non-participation in a structure. Similarly, in this study there was an apparent misalignment between information security interpretive schemes in signification structures and weakly enforced sanctions propagated by legitimisation structures, which had a subsequent influence on compliance behaviour.

6.2.4 Information Security Policies and Compliance Behaviour - Perspective of Implementers and Employees

This section discusses the enacted structures in the process of ISP implementations, and the effect on information security compliance behaviour. Given that ISPs are a form of exerting power over resources (Dhillon & Backhouse, 2001), it therefore means that both management and information security personnel have the power to influence ISPs in the technology domain. Furthermore, it has been established that structures of domination are enacted where parent organisations have authoritative power to dictate ISPs to be implemented within subsidiaries (Giddens, 1984). This domination structure subsequently aids a security team in legitimising the acquisition of funds as an allocative resource for ISP implementations (McPhee, et al., 2016). Security personnel then use their professional expertise as an authoritative resource to facilitate ISP implementations (Andersson, et al., 2022), albeit at the behest of their parent organisation. Prior research has shown that similar domination structures within multinationals could have an adverse effect on ISP diffusion and acceptance in subsidiary organisations, which is corroborated by this study's findings (Yayla & Lei, 2018).

The reflexive monitoring of information security personnel within a multinational consequently creates the impression that security initiatives are imposed on them, and that they have little control over ISP implementations, as portrayed in Figure 11. This is an unintended consequence of the enacted structures of domination, as implementers are granted limited opportunities to contribute to ISP decision making. Information security personnel, who are generally ISP implementors, subsequently perceive a lack of confidence in their professional ability. In addition, the structure of domination enacted within a multinational typically portrays a lack of trust in the implementer's knowledgeability of their organisational

and cultural context. The degree of trust exhibited is also a reflection of the perceived strength of organisational support towards implementers, which research shows can have a negative effect on compliance behaviour (D'Arcy & Greene, 2014). Organisational support is defined as the perceived degree to which an organisation is concerned about the well-being and contributions of their employees (Rhoades & Eisenberger, 2002). A lack of autonomy afforded to ISP implementers and their perceived lack of control over ISPs, which is their professional responsibility, is an indication of the degree of organisational support. The greater the perceived organisational support, the greater their commitment and job involvement (Rhoades & Eisenberger, 2002). Similarly, increased trust exhibited by an organisation should strengthen the reciprocal obligations of implementers, as well as improve their sense of ownership and responsibility (Workman, 2009; Menard, Warkentin, & Lowry, 2018). Reciprocal trust, between implementers and the multinational organisation, is also cited as a key factor in creating a cyber security culture (Uchendu, Nurse, Bada, & Furnell, 2021).

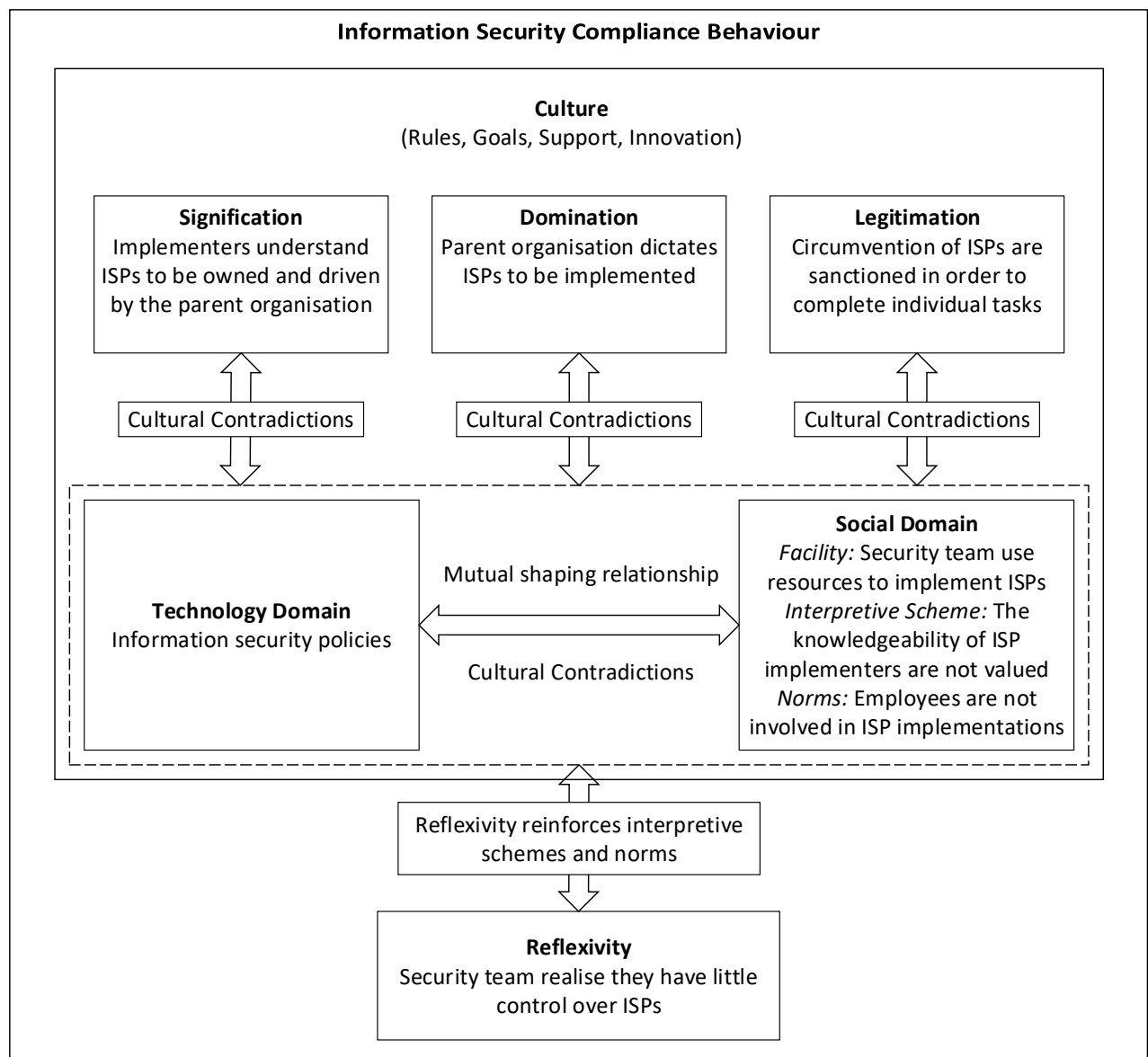


Figure 11. Information Security Policies and Compliance Behaviour of Implementers

Implementers subsequently draw on interpretive schemes in the social domain which communicates a devaluing of their shared stocks of knowledge. When an organisation devalues the knowledgeability of agents, implementers are less committed to the ISPs they implement, which are deemed to be forced upon them by their parent organisation. This creates a sense of indifference among ISP implementers, which in turn has a negative influence on the diffusion of their role responsibilities (Faily & Fléchais, 2010). As a result, structures of signification are reinforced in the minds of implementers, which reflects an understanding that ISPs are owned and exerted by their parent organisation.

The enacted signification structure within a multinational during ISP implementations essentially shapes how ISPs are implemented in the technology domain, of which an unintended consequence is a lack of collaboration and employee involvement in ISP implementations. Security researchers and practitioners generally recommend a collaborative approach to ISPs, where employees are actively involved in the process of ISP development and implementation (Arhin & Wiredu, 2018; Nasir, et al., 2019; Karjalainen, et al., 2020; Yoo, Goo, & Rao, 2020). For example, several researchers who utilised Social Bond Theory to interrogate the compliance behaviour phenomenon, found social ties to be a strong predictor for information security compliance behaviour (Ifinedo, 2014; Dong, Ali, Dominic, & Ali, 2021). A core tenet of Social Bond Theory is employee involvement in particular activities, which in this case is ISPs (Safa, Maple, Watson, & Furnell, 2018). Organisations can therefore use methods of collaboration as an intervention to strengthen employee social ties with ISPs, and thereby improve compliance behaviour. Additionally, an unintended consequence of the enacted domination structures in the process of ISP implementations, is the production of legitimisation structures in the minds of implementers, where ISP circumvention is sanctioned in order to complete individual tasks. The lack of commitment from implementers, and the inconvenience of ISPs, provides both the reasoning and justification in legitimisation structures for non-compliant behaviour.

The structures enacted in the implementation of ISPs within a multinational also have unintended consequences on the compliance behaviour of employees. A finding in structurational analysis is the effects of contradictions on employee perceptions of information security, and subsequent compliance behaviour, as depicted in Figure 12. There is a clear sense of frustration among employees when experiencing the effects of cultural contradictions and conflict in their daily norms. Previous research has shown that conflict of this kind can stimulate negative emotional responses to ISPs among employees (Chen, et al., 2021). Negative emotional responses also have an adverse effect on the reciprocal trust between ISP implementers and employees, which according to Uchendu et al. (2021), stifles the cultivation of a security compliant culture. This study show that employees unanimously agree that ISPs impede their productivity, performance, and ability to innovate, which is essentially an outcome of reflexive monitoring. This finding confirms research, where employees generally perceive ISPs to impede their performance (Bulgurcu, et al., 2010; Hwang, et al., 2017; Karjalainen, et al., 2020). This view is found to be most cogent among management and senior professionals within an IS department. This could be due to the need

for them to collaborate with security personnel and work closer together on IS projects. Professionals in the IS industry are also generally more affected by ISPs, due to their privileged access to IS and elevated permissions (Torten, Reaiche, & Boyle, 2018). Given the recommendation of employee involvement in ISP implementations (Nasir, et al., 2019; Karjalainen, et al., 2020; Yoo, et al., 2020), it is logical to consider proportionally greater involvement of IS professionals as they are more affected by ISPs, and therefore require greater motivation to comply.

As represented in Figure 12, ISP implementations within a multinational also have unintended consequences on employee compliance behaviour. Employees reflexively monitor the security team's response to the apparent contradictions they experience, which can be interpreted as expecting reflexivity from their peers (Walsham, 2002; Andersson, et al., 2022). Reflexivity from ISP implementers would signal an effort to align policies implicated in contradictions, and minimise disruptions to the daily practices of employees. Implementors however, with a sense of being undervalued by their organisation, enact structures of signification and legitimation which demonstrate an indifference to the unintended consequences of ISPs. The perceived lack of reflexivity from ISP implementers is deemed to contradict a goal-oriented organisation, where cultural values of collaboration, innovation, and accountability are emphasised (Van Muijen, et al., 1999). Thus, the observed normative behaviour of ISP implementers, contradicts the cultural values and norms purported by a goal-oriented organisation that encourages innovation. Additionally, the perceived lack of reflexivity from implementers further diminishes reciprocal trust with employees. As a result, employees draw on interpretive schemes in the social domain, which communicates that ISP implementers are uninterested in understanding the daily practices and associated business needs.

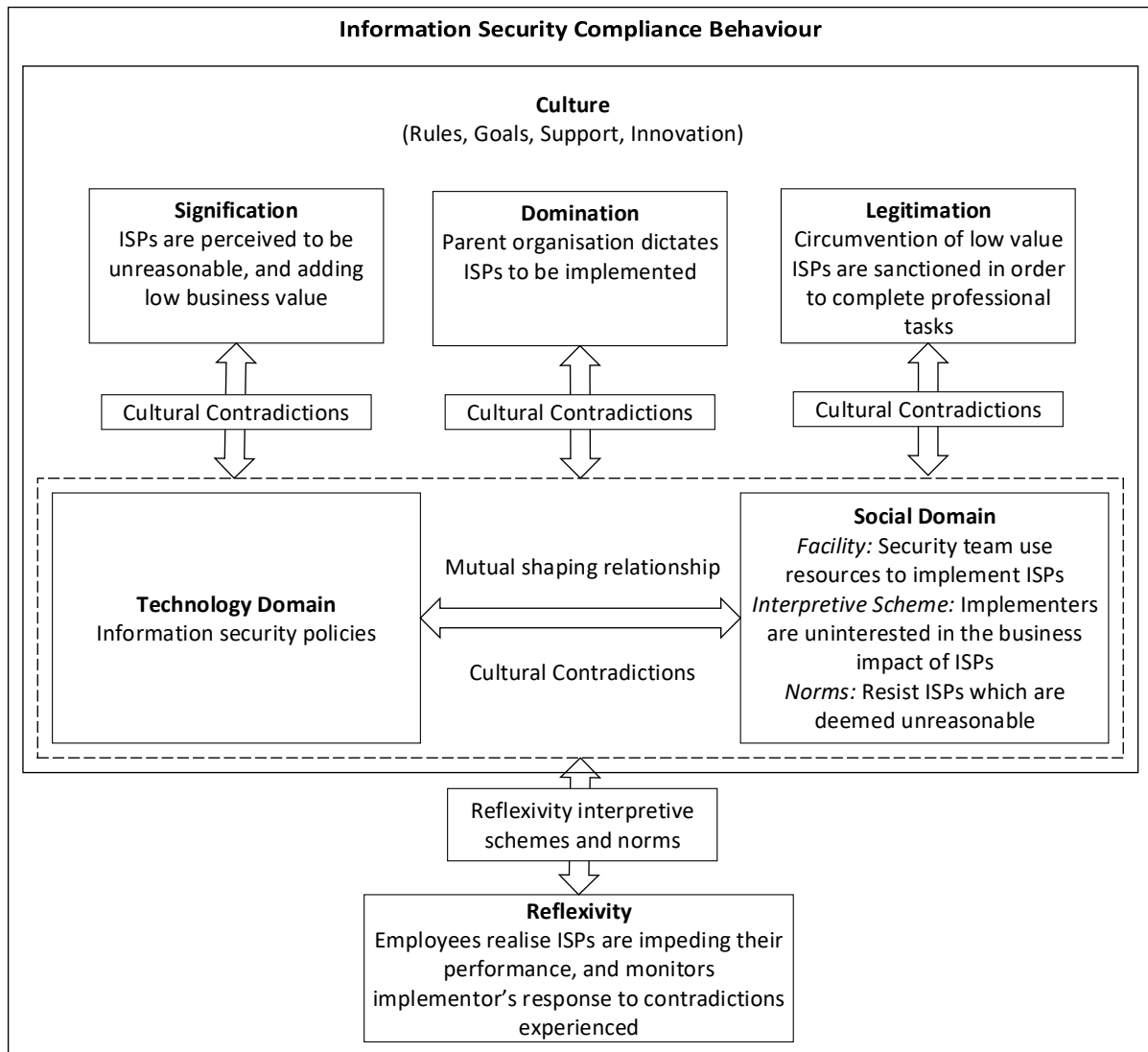


Figure 12. Information Security Policies and Compliance Behaviour of Employees

The adverse impact of ISPs on professional goal achievement, combined with the perceived contradictory response from implementers, are found to leave employees questioning the legitimacy of ISPs. This corroborates prior research which argues that employee perceptions of the legitimacy of ISPs is a key predictor for compliance behaviour (Hu, et al., 2012). Researchers therefore encourage organisations to improve employee perceptions of the legitimacy of ISPs (Cram, et al., 2017). Perceived legitimacy is the extent to which employees believe an ISP to be appropriate, proper, and just (Son, 2011). Tyler (2006) argued that legitimacy is important to the success of those in authority, for “when it is possessed, leads people to defer voluntarily to decisions, rules, and social arrangements” (Tyler, 2006, p. 376). Additionally, Cram, et al. (2017) showed that employee perceptions on whether ISPs are legitimate, fair, and reasonable is a strong determinant of compliance behaviour. While

legitimacy alone might not guarantee compliance, it could however mitigate negative perceptions, as the impact of contradictions could lead employees to deem ISPs in the technology domain as unfair and unreasonable. This study shows that employees generally view ISPs which conflict with their daily practices as unreasonable, and resist compliance to those policies. Thus, instead of ISPs being exhibited as an enabler as research suggests (Damenu & Beaumont, 2017; Karanja, 2017), they are perceived as an inhibitor that adds low business value to the organisation.

The interpretive scheme and norm in the social domain that employees draw on shapes how they interact and use technology (Bernardi, 2017). This mutual shaping ultimately produces signification structures in the minds of employees, where ISPs are understood to be a hinderance and unreasonable, adding low business value to the organisation. Associated legitimation structures are subsequently produced in the minds of employees, where ISPs are circumvented in experiences of conflict in order to complete professional tasks. This finding confirms the assertion in research that employees typically bypass ISPs when they conflict with their daily practices (Hwang & Oona, 2018; Li, et al., 2020; Cram, et al., 2021). However, a structural analysis of antecedents to cultural contradictions, conflict and ensuing compliance behaviour is a novel contribution to our knowledge.

Furthermore, Walsham (2002) showed how the reflexivity of subordinates during conflicting experiences can lead them to exercise power over their superiors by choosing not to comply. This is what Giddens (1984) referred to as the dialectic of control, where all actors have some measure of power to reinforce or change their social structures. Similarly, this study's findings show that employees exert a measure of power to control their own social domain, by deciding to disregard ISPs in the technology domain when they contradict and conflict with their professional norms and goals. The continuous non-compliance of employees in the social domain inevitably leads to further ISPs, resulting in changes in the technology domain. Extant literature confirms that employees are likely to subvert ISPs if they are deemed to inconvenience them and hinder their own productivity (Hwang, et al., 2017; Karjalainen, et al., 2020). This subsequently reproduces the justification for information security non-compliant behaviour in structures of legitimation.

Structurational findings in this study show that poorly contextualised information security training can contradict an organisation's security goals, which reinforces normative behaviour of non-compliance. In addition, findings also show how unaligned information

security goals can lead to contradictory structures of signification, which result in norms of non-compliance to ISPs. Moreover, this study explains how ISP implementations can intensify the negative effect of cultural contradictions and conflict on compliance behaviour. This is a novel finding, as few studies have investigated contradictions and compliance behaviour from a value-based and cultural perspective, but to our knowledge not from a social structure perspective (Karlsson, et al., 2015). Furthermore, results also show the distinct challenges that could arise with the implementation of ISPs within a multinational organisation.

In summary, Table 11 outlines the structural contradictions that are implicated during the process of ISP compliance behaviour. The contradictions are based on differences in structural properties which, if they contain a degree of systemness, are conceptualised as shared by a group and culture (Walsham, 2002). All four cultural contradictions, as proposed by Geeling, et al. (2020) and described in Table 10, namely Priority Contradictions, Process Contradictions, Vision Contradictions, and Technology Contradictions are unintended consequences of or antecedent to enacted structures.

Table 11. Cultural Contradictions Implicated in Enacted Structures of Compliance Behaviour

Structural Contradictions	Enacted Structures	Cultural Contradictions Implicated in Compliance Behaviour
- Can occur when there are divisions of interest between individuals or groups (Giddens, 1984), and between values embedded in technology and those held by social actors (Walsham, 2002). - Structural properties can resemble enough systemness to be regarded	Information Security Training and Compliance Behaviour	Training content is misaligned with ISPs. As a result, employees draw on an interpretive scheme which contradicts the interpretive schemes embedded in ISPs, leading to an understanding that compliance is negotiable and secondary to productivity. Forms of Priority Contradictions, Process Contradictions, and Technology Contradictions are implicated.
	Information Security Goals and Compliance Behaviour	Information security goals embedded in technology contradict the professional goals of employees. ISPs are circumvented to achieve

as shared by a group and culture (Walsham, 2002).		professional goals. Employees comply with ISPs only when they do not impede professional goals. Forms of Vision Contradictions are implicated.
	Information Security Sanctions and Compliance Behaviour	A uniform approach to ISPs infuses contradictions and conflict within a multinational organisation, leading to weakly enforced sanctions which are misaligned with strictly defined ISPs. Compliance to ISPs is understood to be optional, while the completion of professional tasks are obligatory. Forms of Priority Contradictions, Process Contradictions, Technology Contradictions, and Vision Contradictions are implicated.
	Information Security Policies and Compliance Behaviour of Implementors	Domination structures which undermine the knowledgeability of security professionals, infuse contradictory signification and legitimization structures, leading to an indifference and lack of commitment to ISPs. Non-compliance to ISPs is justified to complete individual tasks. Forms of Priority Contradictions, Process Contradictions, Technology Contradictions, and Vision Contradictions are implicated.
	Information Security Policies and Compliance Behaviour of Employees	When implementer indifference to the effect of ISPs contradicts the cultural values of an organisation, a negative response towards ISPs is evoked among employees. Employees will perceive ISPs to be unreasonable and adding low

	business value, which justifies their non-compliance to complete professional tasks. Forms of Priority Contradictions, Process Contradictions, Technology Contradictions, and Vision Contradictions are implicated.
--	---

7 Conclusions

Securing information assets with information security technology remains a priority for organisations (Kappelman, et al., 2017; Robbins & Secholer, 2018). However, the compliance behaviour of employees is found to be the greatest weakness in an organisation's information security defence (AlHogail, 2015). Cultivating an information security culture is postulated to be an effective means of addressing the weakness of employee compliance behaviour (Da Veiga & Martins, 2017). However, instilling a culture where information security compliance behaviour is second nature is a challenge. Information security culture values are often in contradiction with employee espoused values, which inevitably lead to conflict and non-compliant behaviour (Kolkowska, 2011).

The impact of cultural contradictions and conflict on the information security compliance behaviour of employees has received limited attention from researchers (Karlsson, et al., 2018; Yayla & Lei, 2018). Furthermore, extant research addressing the phenomenon has predominantly relied on value-based theoretical frameworks originating from organisational science, which led to the recommendation for supplementary social theories to be used instead (Karlsson, et al., 2015). This study endeavoured to address this limitation by adopting structuration theory as a sensitising lens to provide empirical insights into how cultural contradictions effect information security compliance behaviour.

Contradictions between the espoused values of employees and the security values underpinning technology, priorities, processes, and vision were found to be rife, and are shown to have an adverse effect on compliance to ISPs. This finding therefore confirms Geeling, et al. (2020) depiction of cultural contradictions present in IS projects, by showing evidence of its occurrence in the process of information security compliance behaviour. Thus, this study succeeded in answering the secondary research questions pertaining to the level of compliance behaviour, as well as identifying the various contradictions that emerge.

In answering the primary research question, a structural analysis showed how ineffective information security awareness training can lead to contradictory information security interpretive schemes, which results in norms of non-compliance. Appropriate information security training is imperative to increase employee awareness and understanding of policies, and thereby mitigate experiences of cultural contradictions and their effects on compliance behaviour (Xu & Guo, 2019). Failure to improve employee knowledge of ISPs through

contextualised training, essentially contributes to contradictory interpretive schemes about security and makes cultivating a security compliant culture a challenge (Dhillon, et al., 2016). In addition, the findings showed that a misalignment of security goals can cause a deficiency in employee understanding of information security risks, and contribute to contradictory security interpretive schemes, which results in norms of non-compliance. Failure to align information security goals will ultimately hinder the organisation's common goal of compliance behaviour among employees (Hwang, et al., 2017).

Furthermore, this study's structural analysis provided insights into the contradictions that emerge during ISP implementations within a multinational organisation. The emerging contradictions between ISPs and the professional tasks of employees lead to conflicting priorities, which results in undesirable norms of non-compliance. In addition, employees generally monitor the compliance behaviour of their peers and observe a lack of consequences, which further contributes negatively to compliance norms (D'Arcy, et al., 2009; Tsohou, et al., 2015; Hwang, et al., 2017).

Moreover, this study showed how employee experiences of cultural contradictions and conflict contribute to negative perceptions of information security in general, which to our knowledge is a novel finding. Employees are therefore led to question the legitimacy of ISPs and are more likely to disregard policies when experiencing contradictions (Hu, et al., 2012). Employee perceptions of ISPs is a strong determinant of ensuing compliance behaviour (Cram, et al., 2017). Experiences of ongoing contradictions are found to stimulate negative emotions which further reinforces negative perceptions of information security (Chen, et al., 2021).

7.1 Theoretical Implications

This study successfully answered the primary research question at hand by explaining how cultural contradictions are implicated in the information security compliance behaviour of employees. While the effects of contradictions on compliance behaviour have received little research attention, previous studies have endeavoured to examine the phenomenon (Karlsson, et al., 2018; Yayla & Lei, 2018). However, the subject has primarily been addressed using value-based theoretical frameworks, stemming from organisational science. Hence, Karlsson, et al. (2015) called for the application of complementary theories from social science to examine the implications of contradictions on compliance behaviour. This study addressed

this limitation by using Structuration Theory as its theoretical lens to identify social structures enacted in compliance behaviour, and thereby contributed to the existing body of knowledge. This study also builds upon previous adaptations (Walsham, 2002; Bernardi, 2017) of Structuration Theory in analysing cultural contradictions and IS, and shows how a structural analysis can provide deeper insights into the compliance behaviour phenomenon.

Furthermore, the findings confirm prior research (Geeling, et al., 2020) by providing empirical evidence for Priority Contradictions, Process Contradictions, Technology Contradictions, and Vision Contradictions during information security compliance behaviour.

7.2 Practical Implications

The findings of this study have practical implications for organisations. Firstly, the finding supports prior research and confirms that information security training must be contextualised and appropriate for the organisational context (Parsons et al., 2014; Safa, et al., 2016). To this end, researchers have recommended that organisations try to understand the different motivations and stages of compliance behaviour of employees, and thereby particularise security training accordingly (Karjalainen, et al., 2020). Moreover, contextualised training should include the organisation's information security goals, as it will increase awareness of risks and minimise role ambiguity (McCormac, et al., 2017; Hwang & Oona, 2018). Additionally, organisations should be cognisant of the distinction between information security and cyber security when implementing an information security training programme (von Solms & von Solms, 2018). As an intervention it is therefore recommended that training material should include actual ISP content that is easily understandable, and explicate 'why' a specific policy is needed (Alotaibi, Furnell, & Clarke, 2016; Da Veiga & Martins, 2017).

Secondly, the findings reiterate that a one size fits all approach to implementing ISPs can have a negative effect on compliance behaviour (Alotaibi, et al., 2016). Hence, researchers have presented tools for managers to better understand the rationale behind the compliance behaviour of employees before implementing policies (Kolkowska, Karlsson, & Hedström, 2017). Understanding the values, motivations, and daily norms of employees is imperative if organisations are to overcome the challenges of implementing security policies which impact their daily practices (Hedström, et al., 2011). Additionally, a one size fits all approach to ISP implementations are unfitting within the context of a multinational organisation. The findings showed distinct cultural differences between the parent and subsidiary organisation, which

evidence confirms results in cultural contradictions (Da Veiga & Martins, 2017).

Multinational organisations are therefore best advised to reconsider their approach to ISP implementations (Leidner & Kayworth, 2006), and endeavour to identify the dominant information security culture and subcultures from the outset (Da Veiga & Martins, 2017).

Thirdly, the general tightness and looseness of the cultures should also be considered in a multinational organisation, which has implications on the cultural fit and the effectiveness of rules and sanctions (Gelfand, et al., 2006). It is therefore recommended that strict ISPs should only be considered in a hierarchical culture, where exceptional circumstances are rare, and where employees are not expected to make compliance decisions (Paananen, et al., 2020). Conversely, for goal-oriented cultures who expect employees to seize new opportunities, more loosely defined ISPs with weaker sanctions are recommended. Further to sanctions as a means of deterrence, organisations can use reward enforcement for ISP compliance as an alternative means of motivation (Chen, Ramamurthy, & Wen, 2012).

Fourthly, organisations can improve the perceived legitimacy of ISPs by encouraging knowledge sharing and collaboration with security personnel, and thereby increase acceptance of the social arrangement (Tyler, 2006; Son, 2011; Safa, et al., 2016). Increased collaboration and employee involvement in turn lead to stronger social ties in the social domain, and shape interactions with the technology which favours compliance to ISPs (Safa, et al., 2018; Dong, et al., 2021).

Lastly, findings also illustrate that when ISPs hinder the daily practices of employees, negative perceptions of information security are reinforced in interpretive schemes. Albrechtsen and Hovden (2009) pointed out that security and non-security personnel often have different views on information security. They also generally have limited interaction with one another which augments a lack of understanding of each other's views. This lack of understanding contributes to organisations implementing ISPs which are not aligned with the daily business practices of employees. It is therefore recommended that organisations try to understand the contradictions employees are experiencing, their associated feelings, and introduce appropriate interventions to regulate those experiences (Lowry, Cao, & Everard, 2011). As Safa et al. (2015) stated, "Information security management should consider users and their perceptions as important factors to provide a secure environment. In other words, users are the centre of the security concept." (Safa et al., 2015, p. 66).

7.3 Limitations

Like most things, this study is not without limitations. Firstly, the cross-sectional timeframe of this study inhibited the researcher from observing whether contradictions will eventually lead to a compromise over time. Secondly, because the data collection phase occurred during a pandemic, all interviews were conducted virtually, which means the interviewer had to forgo the benefit of observing body language and other gestures (Bhattacharjee, 2012). Lastly, the research sample was adequate but not ideal. Of the 18 interviewees, only 3 held positions in a non-IT department. A larger sample with greater variation would have been better.

7.4 Recommendations for Future Research

The aspect of ISP implementations within a multinational organisation requires further attention. Future research could interrogate practical considerations for multinational organisations before and after ISP implementations, so as to minimise the disruption to the daily practices of employees. Additionally, future studies of this nature could also do a comparison of structural analysis and cultural analysis results between the parent and subsidiary organisation. A multiple case study in general could also facilitate comparisons to be drawn, which could provide further insights into cultural contradictions and its influence on compliance behaviour.

Furthermore, while this study showed how cultural contradictions influences information security compliance behaviour, there is potentially several other antecedents to non-compliance behaviour. To that end, future studies could investigate how unsanctioned workarounds influence information security compliance behaviour. Similar, change management could be both an antecedent and a consequence of cultural contradictions, the interrogation of which could provide a supplementary contribution.

While this study relied on Structuration Theory to underpin its interrogation, future studies could use alternative perspectives, such as critical realism. An alternative perspective on the interplay between structure and agency could further advance an understanding of the phenomenon.

8 References

- Adams, A., & Sasse, A. M. (1999). Users Are Not the Enemy. *Communications of the ACM*, 42(12), 40-46. doi:10.1145/322796.322806
- Albrechtsen, E., & Hovden, J. (2009). The Information Security Digital Divide Between Information Security Managers and Users. *Computers & Security*, 28(6), 476-490. doi:10.1016/j.cose.2009.01.003
- AlHogail, A. (2015). Design and Validation of Information Security Culture Framework. *Computers in Human Behavior*, 49, 567-575.
- Alhojailan, M. I. (2012). Thematic Analysis: A Critical Review of its Process and Evaluation. *West East Journal of Social Sciences*, 1(1), 39-47.
- Alotaibi, M., Furnell, S., & Clarke, N. (2016). Information Security Policies: A Review of Challenges and Influencing Factors. *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, (pp. 352-358). doi:10.1109/ICITST.2016.7856729
- Alvesson, M. (2002). *Understanding Organizational Culture*. California: SAGE.
- Andersson, A., Hedström, K., & Karlsson, F. (2022). Standardizing Information Security – a Structural Analysis. *Information & Management*, 103623.
- Archer, M. S. (1995). *Realist Social Theory: The Morphogenetic Approach*. Cambridge University Press.
- Arhin, K., & Wiredu, G. O. (2018). An Organizational Communication Approach to Information Security. *The African Journal of Information Systems*, 10(4), 261-279.
- Azjen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211. doi:doi.org/10.1016/0749-5978(91)90020-T
- Bacharach, S. B. (1989). Organizational Theories: Some Criteria for Evaluation. *The Academy of Management Review*, 14(4), 496-515. doi:10.2307/258555

- Bandura, A. (1977). Self-efficacy: Toward a Unifying Theory of Behavioral Change. *Psychological Review*, 84(2), 191-215.
- Bernardi, R. (2017). Health Information Systems and Accountability in Kenya: A Structuration Theory Perspective. *Journal of the Association for Information Systems*, 18(12), 931-958.
- Bhattacharjee, A. (2012). *Social Science Research: Principles, Methods, and Practices*. (2nd, Ed.) Florida: Global Text Project.
- Boland, R. J. (1985). Accounting and the Reproduction of Culture: Budgets and the Process of Structuration. *European Institute for Advanced Studies in Management*.
- Brannen, M. Y., & Salk, J. E. (2000). Partnering Across Borders: Negotiating Organizational Culture in a German-Japanese Joint Venture. *Human Relations*, 53(4), 451-487. doi:10.1177/0018726700534001
- Braun, V., & Clarke, V. (2006). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, 3(2), pp. 77-101.
- Braun, V., & Clarke, V. (2012). Thematic Analysis. In P. Camic, K. Sher, A. T. Panter, D. Long, D. Rindskopf, & H. Cooper (Ed.), *APA Handbook of Research Methods in Psychology, Vol 2: Research Designs: Quantitative, Qualitative, Neuropsychological, and Biological*. (Vol. 2, pp. 57–71). American Psychological Association. doi:10.1037/13620-004
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS quarterly*, 34(3), 523-548.
- Cameron, K. S., & Quinn, R. E. (2011). *Diagnosing and Changing Organizational Culture: Based on the Competing Values Framework*. San Francisco: John Wiley & Sons.
- Chang, K.-C., & Seow, Y. M. (2014). Effects of IT-culture conflict and user dissatisfaction on information security policy non-compliance: A sensemaking perspective.

- Proceedings of the 20th Americas Conference on Information Systems (AMCIS)*, (pp. 1-12).
- Chang, S. E., & Lin, C.-S. (2007). Exploring Organizational Culture for Information Security Management. *Industrial Management & Data Systems*, 107(3), 438-458.
- Chen, H., Li, Y., Chen, L., & Yin, J. (2021). Understanding Employees' Adoption of the Bring-Your-Own-Device (BYOD): The Roles of Information Security-Related Conflict and Fatigue. *Journal of Enterprise Information Management*, 34(3), 770-792. doi:10.1108/JEIM-10-2019-0318
- Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X., Moody, G. D., & Willison, R. (2021). Understanding Inconsistent Employee Compliance with Information Security Policies Through the Lens of the Extended Parallel Process Model. *Information Systems Research*, 32(3), 1043-1065. doi:10.1287/isre.2021.1014
- Chen, Y., Ramamurthy, K. (., & Wen, K.-W. (2015). Impacts of Comprehensive Information Security Programs on Information Security Culture. *Journal of Computer Information Systems*, 55(3), 11-19.
- Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems*, 29(3), 157-188. doi:10.2753/MIS0742-1222290305
- Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the Violation of IS Security Policy in Organizations: An Integrated Model Based on Social Control and Deterrence Theory. *Computers & Security*, 39, 447-459.
- Connaughton, S. L., & Shuffler, M. (2007). Multinational and Multicultural Distributed Teams: A Review and Future Agenda. *Small Group Research*, 38(3), 387-412. doi:10.1177/1046496407301970
- Cram, A. W., Proudfoot, J. G., & D'Arcy, J. (2021). When Enough is Enough: Investigating the Antecedents and Consequences of Information Security Fatigue. *Information Systems Journal*, 31(4), 521-549. doi:10.1111/isj.12319

- Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019, June). Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly*, 43(2), 525-554.
- Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational Information Security Policies: A Review and Research Framework. *European Journal of Information Systems*, 26(6), 605–641.
- Da Veiga, A. (2016). A Cybersecurity Culture Research Philosophy and Approach to Develop a Valid and Reliable Measuring Instrument. *Proceedings of 2016 SAI Computing Conference (SAI)* (pp. 1006-1015). London, UK: IEEE.
doi:10.1109/SAI.2016.7556102
- Da Veiga, A., & Eloff, J. (2010). A Framework and Assessment Instrument for Information Security Culture. *Computers & Security*, 29(2), 196-207.
- Da Veiga, A., & Martins, N. (2015). Improving the Information Security Culture Through Monitoring and Implementation Actions Illustrated Through a Case Study. *Computers & Security*, 49, 162-176.
- Da Veiga, A., & Martins, N. (2017). Defining and Identifying Dominant Information Security Cultures and Subcultures. *Computer & Security*, 70, 72-94.
- Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining Organisational Information Security Culture – Perspectives from Academia and Industry. *Computers & Security*. doi:<https://doi.org/10.1016/j.cose.2020.101713>
- Damenu, T. K., & Beaumont, C. (2017). Analysing Information Security in a Bank Using Soft Systems Methodology. *Information & Computer Security*, 25(3), 240-258.
- D'Arcy, J., & Greene, G. (2014). Security Culture and the Employment Relationship as Drivers of Employees' Security Compliance. *Information Management & Computer Security*, 22(5), 474-489.
- D'Arcy, J., & Teh, P.-L. (2019). Predicting Employee Information Security Policy Compliance on a Daily Basis: The Interplay of Security-Related Stress, Emotions, and

- Neutralization. *Information & Management*, 56(7), 103151.
doi:10.1016/j.im.2019.02.006
- D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, 20(1), 79-98.
- Davison, R. M., & Ou, C. X. (2018). Subverting Organizational IS Policy With Feral Systems: A Case in China. *Industrial Management & Data Systems*, 118(3), 570-588.
doi:10.1108/IMDS-04-2017-0153
- DeSanctis, G., & Poole, S. M. (1994). Capturing the Complexity in Advanced Technology Use: Adaptive Structuration Theory. *Organization Science*, 5(2), 121-147.
doi:10.1287/orsc.5.2.121
- Dhillon, G., & Backhouse, J. (2001). Current Directions in IS Security Research: Towards Socio-Organisational Perspectives. *Information Systems Journal*, 11(2), 127-153.
- Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting Information Security Culture: An Organizational Transformation Case Study. *Computers & Security*, 56, 63-69.
doi:doi.org/10.1016/j.cose.2015.10.001
- Dong, K., Ali, R. F., Dominic, P. D., & Ali, S. E. (2021). The Effect of Organizational Information Security Climate on Information Security Policy Compliance: The Mediating Effect of Social Bonding towards Healthcare Nurses. *Sustainability*, 13(5), 247–257. doi:10.3390/su13052800
- Dubois, A., & Gadde, L.-E. (2002). Systematic Combining: An Abductive Approach to Case Research. *Journal of Business Research*, 55(7), 553-560.
doi:https://doi.org/10.1016/S0148-2963(00)00195-8
- Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *Academy of Management*, 14(4), 532-550.
- Faerman, S. R., & Quinn, R. E. (1985). Effectiveness: The Perspective from Organizational Theory. *The Review of Higher Education*, 9(1), 83-100. doi:10.1353/rhe.1985.0006

- Faily, S., & Fléchais, I. (2010). Designing and Aligning e-Science Security Culture With Design. *Information Management & Computer Security*, 18(5), 339-349.
doi:10.1108/09685221011095254
- Festing, M., & Maletzky, M. (2011). Cross-Cultural Leadership Adjustment — A Multilevel Framework Based on the Theory of Structuration. *Human Resource Management Review*, 21(3), 186-200. doi:/10.1016/j.hrmr.2011.02.005
- Flores, W. R., & Ekstedt, M. (2016). Shaping Intention to Resist Social Engineering Through Transformational Leadership, Information Security Culture and Awareness. *Computers & Security*, 59, 26–44.
- Gartner. (2018). *Gartner Forecasts Worldwide Information Security Spending to Exceed \$124 Billion in 2019*. Gartner. Retrieved from <https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019>
- Gartner. (2018). *Security and Engineering — Converging or Colliding?* Gartner. Retrieved March 20, 2022
- Gartner. (2021). *Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed \$150 Billion in 2021*. Retrieved from <https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem>
- Geeling, S. L., Brown, I., & Weimann, P. (2020). Cultural Levels and Emergent Cultural Contradictions in IS Development. In *Proceedings of the 28th European Conference on Information Systems (ECIS)*. An Online AIS Conference.
- Geeling, S., Brown, I., & Weimann, P. (2017). Processes of Relating: Cultural Implications Information Systems Development. *Preceedings of the Thirty Eighth International Conference on Information Systems*. AIS.
- Gelfand, M. J., Erez, M., & Aycan, Z. (2006). Cross-Cultural Organizational Behavior. *Annual Review of Psychology*, 58(1), 479-514.

- Gelfand, M. J., Nishii, L. H., & Raver, J. L. (2006). On the Nature and Importance of Cultural Tightness–Looseness. *Journal of Applied Psychology*, 91(6), 1225–1244.
- Giddens, A. (1979). *Central Problems in Social Theory: Action, Structure and Contradiction in Social Analysis*. Macmillan Education, Limited.
- Giddens, A. (1984). *The Constitution of Society: Outline of the Theory of Structuration*. United States: University of California Press.
- Gregor, S. (2006). The Nature of Theory in Information Systems. *MIS Quarterly*, 30(3), 611-642.
- Guo, K. H., Yuan, Y., Archer, N., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems*, 28(2), 203-236.
- Haeussinger, F., & Kranz, J. (2017). Antecedents of Employees' Information Security Awareness - Review, Synthesis, and Directions for Future Research. *In Proceedings of the 25th European Conference on Information Systems (ECIS)* (pp. 1-19). Guimarães, Portugal: AIS Electronic Library (AISeL).
- Halperin, R., & Backhouse, J. (2007). Using Structuration Theory in IS Research: Operationalizing Key Constructs. *International Conference on Information Systems 2007 Proceedings* (pp. 1-17). Montreal: AIS Electronic Library.
- Hassan, N. R. (2018). Reinterpreting the Kuhnian Paradigm in Information Systems. *Journal of the Association for Information Systems*, 19(7), 568-599.
- Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. (2011). Value Conflicts for Information Security Management. *Journal of Strategic Information Systems*, 20(4), 373–384.
- Hofstede, G. (1980). Culture and Organizations. *International Studies of Management & Organization*, 10(4), 15-41.
- Hofstede, G. (2011). Dimensionalizing Cultures: The Hofstede Model. *Online Readings in Psychology and Culture*, 2(1), 8.

- Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and Organizations: Software of the Mind: Intercultural Cooperation and its Importance for Survival*. (3rd ed.). London: McGraw-Hill.
- Hsu, C., Backhouse, J., & Silva, L. (2014). Institutionalizing Operational Risk Management: An Empirical Study. *Journal of Information Technology*, 29, 59–72. doi:doi:10.1057/jit.2013.15
- Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies : The Critical Role of Top Management and Organizational Culture. *Decision Sciences*, 43(4), 615-659.
- Hwang, I., & Oona, C. (2018). Examining Technostress Creators and Role Stress as Potential Tthreats to Employees' Information Security Compliance. *Computers in Human Behavior*, 81, 282-293. doi:10.1016/j.chb.2017.12.022
- Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why Not Comply With Information Security? An Empirical Approach for the Causes of Non-Compliance. *Online Information Review*, 41(1), 2-18. doi:10.1108/OIR-11-2015-0358
- Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2021). Security Awareness: The First Step in Information Security Compliance Behavior. *Journal of Computer Information Systems*, 61(4), 345-356. doi:10.1080/08874417.2019.1650676
- Ifinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers & Security*, 31(1), 83-95. doi:10.1016/j.cose.2011.10.007
- 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.
- Indeje, W. G., & Zheng, Q. (2010). Organizational Culture and Information Systems Implementation: A Structuration Theory Perspective. *Sprouts: Working Papers on Information Systems*, 10(27).

- ISO. (2014). *ISO/IEC 27000:2014 Information technology – Security techniques – Information security management systems overview and vocabulary*. International Organization for Standardization (ISO). Technical Report.
- Jahoda, G. (2012). Critical Reflections on Some Recent Definitions of “Culture”. *Culture & Psychology*, 18(3), 289–303. doi:10.1177/1354067X12446229
- Jeffries, M., Phipps, D., Howard, R. L., Avery, A., Rodgers, S., & Ashcroft, D. (2017). Understanding the Implementation and Adoption of an Information Technology Intervention to Support Medicine Optimisation in Primary Care: Qualitative Study Using Strong Structuration Theory. *BMJ Open*, 5, 1-10. doi:10.1136/bmjopen-2016-014810
- Jones, M. R., & Karsten, H. (2008). Giddens's Structuration Theory and Information Systems Research. *MIS Quarterly*, 32(1), 127-157.
- Jones, M., Orlikowski, W., & Munir, K. (2004). Structuration Theory and Information Systems: A Critical Reappraisal. In J. Mingers, & L. Willcocks (Eds.), *Social Theory and Philosophy for Information Systems* (pp. 297-328). West Sussex: John Wiley & Sons Ltd.
- Kabanda, S., & Brown, I. (2017). A structuration analysis of Small and Medium Enterprise (SME) adoption of E-Commerce: The case of Tanzania. *Telematics and Informatics*, 34(4), 118-132. doi:doi.org/10.1016/j.tele.2017.01.002
- Kaplan, B., & Maxwell, J. A. (2005). Qualitative Research Methods for Evaluating Computer Information Systems. In *Evaluating the Organizational Impact of Healthcare Information Systems* (pp. 30-55). New York: Springer.
- Kappelman, L. A., McLean, E. R., Johnson, V. L., Torres, R., Maurer, C., Kim, K., . . . Snyder, M. (2021). The 2020 SIM IT Issues and Trends Study. *MIS Quarterly Executive*, 69-107.
- Kappelman, L., Johnson, V., Maurer, C., McLean, E., Torres, R., David, A., & Nguyen, Q. (2017). The 2017 SIM IT Issues and Trends Study. *MIS Quarterly Executive*, 17(1), 53-88.

- Karahanna, E., Evaristo, R. J., & Srite, M. (2005). Levels of Culture and Individual Behavior: An Integrative Perspective. *Journal of Global Information Management*, 13(2), 1-20.
- Karanja, E. (2017). The Role of the Chief Information Security Officer in the Management of IT Security. *Information & Computer Security*, 25(3), 300-329. doi:2017
- Karjalainen, M., Siponen, M., & Sarker, S. (2020). Toward a Stage Theory of the Development of Employees' Information Security Behavior. *Computers & Security*, 93, 101782. doi:10.1016/j.cose.2020.101782
- Karlsson, F., Åström, J., & Karlsson, M. (2015). Information Security Culture - State-of-the-Art Review Between 2000 and 2013. *Information & Computer Security*, 23(3), 246-285.
- Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based Discourse Analysis of Information Security Policies. *Computers & Security*, 67, 267-279. doi:10.1016/j.cose.2016.12.012
- Karlsson, F., Karlsson, M., & Åström, J. (2017). Measuring Employees' Compliance – The importance of Value Pluralism. *Information & Computer Security*, 25(3), 279-299. doi:<https://doi.org/10.1108/ICS-11-2016-0084>
- Karlsson, M., Denk, T., & Åström, J. (2018). Perceptions of Organizational Culture and Value Conflicts in Information Security Management. *Information & Computer Security*, 26(2), 213-229.
- Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2022). The Effect of Perceived Organizational Culture on Employees' Information Security Compliance. *Information & Computer Security*, 30(3), 382-401. doi:10.1108/ICS-06-2021-0073
- Keutel, M., Michalik, B., & Richter, J. (2014). Towards Mindful Case Study Research in IS: A Critical Analysis of the Past Ten Years. *European Journal of Information Systems*, 23(3), 256-272. doi:10.1057/ejis.2013.26
- Kirlappos, I., Beutement, A., & Sasse, A. M. (2013). "Comply or Die" Is Dead: Long Live Security-Aware Principal Agents. In A. A. Adams, M. Brenner, & M. Smith (Ed.),

Financial Cryptography and Data Security (pp. 70-82). Berlin, Heidelberg: Springer Berlin Heidelberg.

Kissack, H. C., & Callahan, J. L. (2010). The Reciprocal Influence of Organizational Culture and Training and Development Programs: Building the Case for a Culture Analysis Within Program Planning. *Journal of European Industrial Training*, 34(4), 365-380.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, N. F. (2006). Information Security: Management's Effect on Culture and Policy. *Information Management & Computer Security*, 14(1), 24-36. doi:10.1108/09685220610648355

Knights, D., & Willmott, H. C. (1987). Organizational Culture as Management Strategy: A Critique and Illustration from the Financial Services Industry. *International Studies of Management & Organization*, 17(3), 40-63.

Koch, H., Gonzalez, E., & Leidner, D. E. (2011). Resolving IT-Culture Conflict in Enterprise 2.0 Implementations. *Proceedings of the Seventeenth Americas Conference on Information Systems*, (p. Paper 279). Michigan.

Koch, H., Leidner, D. E., & Gonzalez, E. S. (2013). Digitally Enabling Social Networks: Resolving IT-Culture Conflict. *Information Systems Journal*, 23(6), 501–523.

Kolkowska, E. (2011). Security Subcultures in an Organization-Exploring Value Conflicts. *European Conference on Information Systems*, (p. 237).

Kolkowska, E., & De Decker, B. (2012). Analyzing Value Conflicts for a Work-Friendly ISS Policy Implementation. In D. Gritzalis, S. Furnell, & M. Theoharidou (Ed.), *Information Security and Privacy Research* (pp. 339-351). Berlin, Heidelberg: Springer Berlin Heidelberg.

Kolkowska, E., Karlsson, F., & Hedström, K. (2017, March 1). 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. doi:10.1016/j.jsis.2016.08.005

- Kostova, T., & Zaheer, S. (1999). Organizational Legitimacy under Conditions of Complexity: The Case of the Multinational Enterprise. *The Academy of Management Review*, 24(1), 64-81. doi:10.2307/259037
- Kouroubali, A. (2002). Structuration Theory and Conception-Reality Gaps: Addressing Cause and Effect of Implementation Outcomes in Health Care Information Systems. *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, (pp. 1975-1984). doi:10.1109/HICSS.2002.994120
- Kroeber, A. L., & Kluckhohn, C. (1952). *Culture: A Critical Review of Concepts and Definitions*.
- Lee, A. S. (2010). Retrospect and Prospect: Information Systems Research in the Last and Next 25 Years. *Journal of Information Technology*, 25(4), 336-348. doi:10.1057/jit.2010.24
- Leidner, D. E. (2010, February). Globalization, Culture, and Information: Towards Global Knowledge Transparency. *Journal of Strategic Information Systems*, 19(2), 69–77.
- Leidner, D. E., & Kayworth, T. (2006). A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict. *MIS Quarterly*, 30(2), 357-399.
- Li, Y., Pan, T., & Zhang, N. (2020). From Hindrance to Challenge: How Employees Understand and Respond to Information Security Policies. *Journal of Enterprise Information Management*, 33(1), 191-213. doi:10.1108/JEIM-01-2019-0018
- Linton, R. (1945). *The Cultural Background of Personality*. Oxford, England: Appleton-Century.
- Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures. *Journal*, 27(4), 163–200.
- Lowry, P. B., Dinev, T., & Willison, R. (2017). Why Security and Privacy Research Lies at the Centre of the Information Systems (IS) Artefact: Proposing a Bold Research

- Agenda. *European Journal of Information Systems*, 26(6), 546-563.
doi:10.1057/s41303-017-0066-x
- Lyytinen, K. J., & Ngwenyama, O. K. (1992). What Does Computer Support for Cooperative Work Mean? A Structural Analysis of Computer Supported Cooperative Work. *Accounting, Management and Information Technologies*, 2(1), 19-37.
doi:10.1016/0959-8022(92)90007-F
- Markus, H. R., & Kitayama, S. (2010). Cultures and Selves : A Cycle of Mutual Constitution. *Perspectives on Psychological Science*, 5(4), 420–430.
- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual Differences and Information Security Awareness. *Computers in Human Behavior*, 69, 151-156. doi:10.1016/j.chb.2016.11.065
- McPhee, R. D., Poole, M. S., & Iverson, J. (2016). Structuration Theory. In L. L. Putnam, & D. K. Mumby (Eds.), *The SAGE Handbook of Organizational Communication: Advances in Theory, Research, and Methods* (3rd ed., pp. 75-99). SAGE Publications.
doi:10.1002/9781118766804
- Meglino, B. M., & Ravlin, E. C. (1998). Individual Values in Organizations: Concepts, Controversies, and Research. *Journal of Management*, 24(3), 351-389.
- Menard, P., Warkentin, M., & Lowry, P. B. (2018). The Impact of Collectivism and Psychological Ownership on Protection Motivation: A Cross-Cultural Examination. *Computers & Security*, 75, 147-166. doi:10.1016/j.cose.2018.01.020
- Mingers, J., Mutch, A., & Willcocks, L. (2013, September). Critical Realism in Information Systems Research. *MIS Quarterly*, 37(3), 795-802.
- Mironenko, I. A., & Sorokin, P. S. (2018). Seeking for the Definition of Culture: Current Concerns and their Implications. A Comment on Gustav Jahoda's Article "Critical Reflections on some Recent Definitions of 'Culture'". *Integrative Psychological and Behavioral Science*, 52(2), 331–340.

- Mohajan, H. K. (2018). Qualitative Research Methodology in Social Sciences and Related Subjects. *Journal of Economic Development, Environment and People*, 7(1), 23-26.
- Morris, M. W., Williams, K. Y., Leung, K., Larrick, R., Mendoza, M. T., Bhatnagar, D., . . . Hu, J.-C. (1998). Conflict Management Style: Accounting for Cross-National Differences. *Journal of International Business Studies*, 29(4), 729-747.
- Mutudi, M., & Iyamu, T. (2020). An Information Systems Framework to Improve the Issuance of Identity Documents Through Enhanced Data Quality in the Republic of Angola. *The Electronic Journal of Information Systems in Developing Countries*, 86(1), 1-13.
- Myers, M. D., & Tan, F. B. (2002). Beyond Models of National Culture in Information Systems Research. In *Human Factors in Information Systems* (pp. 1-19). Hershey, PA, USA: IGI Global.
- Namey, E., Guest, G., Thairu, L., & Johnstone, L. (2008). Data Reduction Techniques for Large Qualitative Data Sets. In *Handbook for Team-Based Qualitative Research* (Vol. 2, pp. 137-161).
- Nasir, A., Arshah, R. A., Hamid, M. R., & Fahmy, S. (2019). An Analysis on the Dimensions of Information Security Culture Concept: A Review. *Journal of Information Security and Applications*, 12-22.
- Ngwenyama, O., & Nielsen, P. A. (2003, February). Competing Values in Software Process Improvement: An Assumption Analysis of CMM From an Organizational Culture Perspective. *IEEE Transactions on Engineering Management*, 50(1), 100-112.
- Noor, K. (2008). Case Study: A Strategic Research Methodology. *American Journal of Applied Sciences*, 5(11), 1602-1604.
- Ononiwu, C., Brown, I., & Carlsson, S. (2018). Theory Choice In Critical Realist Information Systems Research. *UK Academy for Information Systems Conference Proceedings 2018*, 8.

- Orehek, Š., & Petrič, G. (2020). A Systematic Review of Scales for Measuring Information Security Culture. *Information & Computer Security*, 2056-4961. doi:10.1108/ICS-12-2019-0140
- Orlikowski, W. J. (1992, August). The Duality of Technology: Rethinking the Concept of Technology in Organizations. *Organization Science*, 3(3), 398-427.
- Orlikowski, W. J. (2000). Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations. *Organization Science*, 11(4), 404-428.
- Orlikowski, W. J., & Baroudi, J. J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information systems research*, 2(1), 1-28.
- Paananen, H., Lapke, M., & Siponen, M. (2020). Paananen. *State of the Art in Information Security Policy Development*, 88, 101608. doi:doi.org/10.1016/j.cose.2019.101608
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computer & Security*, 42, 165-176. doi:10.1016/j.cose.2013.12.003
- Peirce, C. S. (1974). *Collected Papers of Charles Sanders Peirce* (Vol. 2). Cambridge, MA: Harvard University Press.
- Poole, M. S., & DeSanctis, G. (2002). Structuration Theory in Information Systems Research: Methods and Controversies. In M. Whitman, & A. Woszczynski (Eds.), *The Handbook of Information Systems Research* (pp. 206-249). IGI Global.
- Pozzebon, M. (2004). The Influence of a Structurationist View on Strategic Management Research. *Journal of Management Studies*, 41(2), 247-272.
- Pozzebon, M., & Pinsonneault, A. (2001). Structuration Theory in the IS Field: An Assessment of Research Strategies. *The 9th European Conference on Information Systems* (pp. 205-217). Bled, Slovenia: Global Co-Operation in the New Millennium.

- Pozzebon, M., & Pinsonneault, A. (2005). Challenges in Conducting Empirical Work Using Structuration Theory: Learning from IT Research. *Organization Studies*, 26(9), 1353-1376.
- PricewaterhouseCoopers. (2018). *Global State of Information Security Survey 2018*. Retrieved May 03, 2020, from pwc:
https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html#title-par_herotitle
- Qu, S. Q., & Dumay, J. (2011). The Qualitative Research Interview. *Qualitative Research in Accounting & Management*, 8(3), 238-264. doi:10.1108/11766091111162070
- Quinn, R. E. (1988). *Beyond Rational Management: Mastering the Paradoxes and Competing Demands of High Performance*. San Fransisco: Jossey-Bass.
- Quinn, R. E., & Rohrbaugh, J. (1983, March). A Spatial Model of Effectiveness Criteria: Towards a Competing Values Approach to Organizational Analysis. *Management Science*, 29(3), 363-377.
- Quinn, R. E., Hildebrandt, H. W., Rogers, P. S., & Thompson, M. P. (1991). A Competing Values Framework for Analyzing Presentational Communication in Management Contexts. *The Journal of Business Communication*, 28(3), 213-232.
- Ramachandran, S., Rao, C., Goles, T., & Dhillon, G. (2013). Variations in Information Security Cultures across Professions: A Qualitative Study. *Communications of the Association for Information Systems*, 33(11), 163–204. doi:10.17705/1CAIS.03311
- Ravishankar, M. N. (2015). The Realignment of Offshoring Frame Disputes (OFD): An Ethnographic ‘Cultural’ Analysis. *European Journal of Information Systems*, 24(3), 234-246. doi:10.1057/ejis.2014.5
- Reid, R., & Van Niekerk, J. (2014). From Information Security to Cyber Security Cultures. *2014 Information Security for South Africa* (pp. 1-7). Johannesburg, South Africa: IEEE. doi:10.1109/ISSA.2014.6950492

- Rhoades, L., & Eisenberger, R. (2002). Perceived Organizational Support: A Review of the Literature. *Journal of Applied Psychology*, 87(4), 698-714. doi:10.1037/0021-9010.87.4.698
- Riley, P. (1983). A Structurationist Account of Political Culture. *Administrative Science Quarterly*, 28(3), 414-437.
- Robbins, J. M., & Sechooler, A. M. (2018). Once More Unto The Breach: What The Equifax And Uber Data Breaches Reveal About The Intersection Of Information Security And The Enforcement Of Securities Laws. *Criminal Justice*, 33(1), 4-7.
- Roberts, R. E. (2020). Qualitative Interview Questions: Guidance for Novice Researchers. *The Qualitative Report*, 25(9), 3185-3203.
- Robey, D. (1995). Theories that Explain Contradiction: Accounting for the Contradictory Organizational Consequences of Information Technology. *ICIS Proceedings* (pp. 55-63). AIS Electronic Library.
- Roccas, S., & Sagiv, L. (2010). Personal Values and Behavior: Taking the Cultural Context into Account. *Social and Personality Psychology Compass*, 4(1), 30–41.
- Rokeach, M. (1973). *The Nature of Human Values*. Free Press.
- Rose, J. (1998). Evaluating the Contribution of Structuration Theory to the Information Systems Discipline. *6th European Conference on Information Systems*, 2, pp. 910-924.
- Rowley, J. (2002). Using Case Studies in Research. *Management Research News*, 25(1), 16-27.
- Rowley, J. (2012). Conducting Research Interviews. *Management Research Review*, 35(3/4), 260-271.
- Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007, February). Organisational Security Culture: Extending the End-User Perspective. *Computers & Security*, 26(1), 56-62.

- Safa, N. S., Maple, C., Watson, T., & Furnell, S. (2018). Motivation and Opportunity Based Model to Reduce Information Security Insider Threats in Organisations. *Journal of Information Security and Applications*, 40, 247-257. doi:10.1016/j.jisa.2017.11.001
- Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information Security Policy Compliance Model in Organizations. *Computers & Security*, 56, 70-82. doi:doi.org/10.1016/j.cose.2015.10.006
- Safa, S. N., Sookhak, M., Von Solms, R., Furnell, S., Ghani, A. N., & Herawan, T. (2015). Information Security Conscious Care Behaviour Formation in Organizations. *Computers & Security*, 53, 65-78. doi:doi.org/10.1016/j.cose.2015.05.012
- Saunders, M., Lewis, P., & Thornhill, A. (2012). *Research Methods for Business Students* (6th ed.). London: Pearson Education.
- Schein, E. H. (1990). Organizational Culture. *American Psychologist*, 45(2), 109-257.
- Schein, E. H. (2010). *Organizational Culture and Leadership*. San Francisco: John Wiley & Sons.
- Schneider, B., Ehrhart, M. G., & Macey, W. H. (2013). Organizational Climate and Culture. *Annual Review of Psychology*, 64, 361-388.
- Schultz, M., & Hatch, M. (1996). Living With Multiple Paradigms the Case of Paradigm Interplay in Organizational Culture Studies. *Academy of Management Review*, 21(2), 529-557.
- Seawright, J., & Gerring, J. (2008). Case Selection Techniques in Case Study Research. *Political research quarterly*, 61(2), 294-308.
- Sewell, W. H. (1992). A Theory of Structure: Duality, Agency, and Transformation. *American Journal of Sociology*, 98(1), 1-29.
- Simon, H. A. (2000). Bounded Rationality in Social Science: Today and Tomorrow. *Mind & Society*, 1(1), 25-39. doi:10.1007/BF02512227

- Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security. *MIS Quarterly*, 34(5), 487-502.
- Smircich, L. (1983). Concepts of Culture and Organizational Analysis. *Administrative Science Quarterly*, 339-358.
- Smith, C. (2016). The Conceptual Incoherence of "Culture" in American Sociology. *The American Sociologist*, 47(4), 388-415.
- Solomon, G., & Brown, I. (2021). The Influence of Organisational Culture and Information Security Culture on Employee Compliance Behaviour. *Journal of Enterprise Information Management*, 34(4), 1203-1228. doi:10.1108/JEIM-08-2019-0217
- Son, J.-Y. (2011). Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to Follow IS Security Policies. *Information & Management*, 48(7), 296-302. doi:10.1016/j.im.2011.07.002
- Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information Security Management Needs More Holistic Approach: A Literature Review. *International Journal of Information Management*, 36(2), 215-225. doi:10.1016/j.ijinfomgt.2015.11.009
- Straub, D., Loch, K., Evaristo, R., Karahanna, E., & Srite, M. (2002). Toward a Theory-Based Measurement of Culture. *Journal of Global Information Management*, 10(1), 12-23.
- Tang, M., Li, M., & Zhang, T. (2016). The Impacts of Organizational Culture on Information Security Culture: A Case Study. *Information Technology and Management*, 17, 179-186.
- Torten, R., Reaiche, C., & Boyle, S. (2018). The Impact of Security Awareness on Information Technology Professionals' Behavior. *Computers & Security*, 79, 68-79. doi:10.1016/j.cose.2018.08.007
- Trang, S., & Brendel, B. (2019). A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research. *Information Systems Frontiers*, 21(6), 1265-1284. doi:10.1007/s10796-019-09956-4

- Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the Introduction of Information Security Awareness Programmes in Organisations. *European Journal of Information Systems*, 24(1), 38–58.
- Tyler, T. R. (2006). Psychological Perspectives on Legitimacy and Legitimation. *Annual Review of Psychology*, 57(1), 375-400. doi:10.1146/annurev.psych.57.102904.190038
- Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a Cyber Security Culture: Current Practices and Future Needs. *Computers & Security*, 109, 102387. doi:10.1016/j.cose.2021.102387
- Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content Analysis and Thematic Analysis: Implications for Conducting a Qualitative Descriptive Study. *Nursing & Health Sciences*, 15(3), 398-405. doi:https://doi.org/10.1111/nhs.12048
- Van Muijen, J. J., Koopman, P., De Witte, K., De Cock, G., Susanj, Z., Lemoine, C., . . . Turnipseed, D. (1999). Organizational Culture : The Focus Questionnaire. *European Journal of Work and Organizational Psychology*, 8(4), 551–568. doi:10.1080/135943299398168
- Van Niekerk, J., & Von Solms, R. (2010). Information Security Culture: A Management Perspective. *Computer & Security*, 29(4), 476-486.
- Vance, A., Siponen, M. T., & Straub, D. W. (2020). Effects of Sanctions, Moral Beliefs, and Neutralization on Information Security Policy Violations Across Cultures. *Information & Management*, 57(4), 103212. doi:10.1016/j.im.2019.103212
- Varpio, L., Paradis, E., Uijtdehaage, P., & Young, M. (2020). The Distinctions Between Theory, Theoretical Framework, and Conceptual Framework. *Academic Medicine*, 95(7), 989-994. doi:10.1097/ACM.0000000000003075
- von Solms, B., & von Solms, R. (2018). Cybersecurity and Information Security – What Goes Where? *Information & Computer Security*, 26(1), 2-9. doi:10.1108/ICS-04-2017-0025

- Walsham, G. (2002). Cross-Cultural Software Production and Use: A Structural Analysis. *MIS Quarterly*, 26(4), 359-380.
- Walsham, G. (2011). *Interpreting Information Systems in Organizations*. Zurich, Switzerland: The Global Text Project.
- Walsham, G., & Han, C.-K. (1990). Structuration Theory and Information Systems Research. *International Conference on Information Systems Proceedings*. 7., (pp. 53-59).
- Weaver, G. R., & Gioia, D. A. (1994). Paradigms Lost: Incommensurability vs Structurationist Inquiry. *Organization Studies*, 15(4), 565-11166.
- Weber, R. (2004). The Rhetoric of Positivism Versus Interpretivism: A Personal View 1. *MIS Quarterly*, 28(1), iii-xii.
- Whetten, D. A. (1989). What Constitutes a Theoretical Contribution? *The Academy of Management review.*, 14(4), 490-495. doi:10.5465/amr.1989.4308371
- Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security* (4th ed.). Boston: Nelson Education, Ltd.
- Whittington, R. (2015). Giddens, Structuration Theory and Strategy as Practice. In *Cambridge Handbook of Strategy as Practice* (pp. 109-126). Cambridge University Press.
- Wiley, A., McCormac, A., & Calic, D. (2020). More Than the Individual: Examining the Relationship Between Culture and Information Security Awareness. *Computers & Security*, 88, 101640. doi:10.1016/j.cose.2019.101640
- Workman, M. (2009). How Perceptions of Justice Affect Security Attitudes: Suggestions for Practitioners and Researchers. *Information Management & Computer Security*, 17(4), 341-353. doi:10.1108/09685220910993999
- Xu, D., & Shenkar, O. (2002). Institutional Distance and The Multinational Enterprise. *Academy of Management Review*, 27(4), 608-618. doi:10.5465/amr.2002.7566108

- Xu, Z., & Guo, K. (2019). It ain't my Business: A Coping Perspective on Employee Effortful Security Behavior. *Journal of Enterprise Information Management*, 32(5), 824-842. doi:10.1108/JEIM-10-2018-0229
- Yammarino, F. J., & Dansereau, F. (2011). Multi-level Issues in Evolutionary Theory, Organization Science, and Leadership. *The Leadership Quarterly*, 22(6), 1042-1057.
- Yayla, A., & Lei, Y. (2018). Information Security Policies and Value Conflict in Multinational Companies. *Information & Computer Security*, 26(2), 230-245.
- Yazdanmehr, A., & Wang, J. (2016). Employees' Information Security Policy Compliance: A Norm Activation Perspective. *Decision Support Systems*, 92, 36-46. doi:doi.org/10.1016/j.dss.2016.09.009
- Yin, R. K. (2009). *Case Study Research: Design and Methods* (4th ed.). SAGE Publications.
- Yoo, C. W., Goo, J., & Rao, H. R. (2020). Is Cybersecurity a Team Sport? A Multilevel Examination of Workgroup Information Security Effectiveness. *MIS Quarterly*, 44(2), 907-931. doi:10.25300/MISQ/2020/15477
- Zaidman, N., Schwartz, D. G., & Te'eni, D. (2008). Challenges to ICT Implementation in Multinationals. *Education, Business and Society: Contemporary Middle Eastern Issues*, 1(4), 267-277. doi:10.1108/17537980810929984

Appendix A. Interview Guide

Participant	
Name	
Division	
Department	
Team	
Duration	

Structure	No.	Question Guide	Research Question
Interpretive Schemes	1	What is the role of information security in the organisation in your view?	RQ1, RQ2
	2	What information security risks are present in your day-to-day work?	RQ1, RQ2
	3	What information security rule / policy is most appropriate in your day-to-day activities?	RQ1, RQ2
Facility	4	How reasonable are the sanctions associated with a given infosec policy violation?	RQ1, RQ2
	5	Do you believe information security policies are an information security team initiative, or a top management initiative?	RQ1, RQ2
Norms	6	Can you give examples where others conformed to appropriate information security rules of behaviour? Ask for examples	RQ1, RQ2
	7	Can you give examples where significant others or managers conform to the appropriate information security rules of behaviour?	RQ1, RQ2
Culture	No.	Question Guide	Research Question
Clan/Support	1	Can you share examples of how your team builds trust among team members?	RQ1, RQ3
Market/Goal	2	In terms of your performance, what is the role of goal-setting in your team?	RQ1, RQ3
	3	Are those goals specified by you or management?	RQ1, RQ3
Adhocracy/Innovative	4	What is the importance of being creative and innovative within your team?	RQ1, RQ3
	5	Can you share examples of when you or your team invested in new products?	RQ1, RQ3
Hierarchical/Rules	6	What is the role of formal procedures and governance in your day-to-day tasks?	RQ1, RQ3
Management & Decision-Making Style	7	How would you characterise the management style in your team?	RQ1, RQ3
	8	And in your organisation?	RQ1, RQ3

Contradictions	No	Question Guide	Research Question
Priority Contradictions	1	What priority do you believe should be given to information security in your day-to-day tasks?	RQ1, RQ3
Process Contradictions	2	What changes have you or your team needed to make in your day-to-day practices to accommodate information security requirements?	RQ1, RQ3
Role Contradictions	3	Who do you think should be responsible for information security in the organisation?	RQ1, RQ3
Vision Contradictions	4	What are some of the information security goals of the organisation?	RQ1, RQ3
	5	How does your team goals align, or misalign, with information security goals?	RQ1, RQ3
Technology Contradictions	6	Can you give examples of when information security policies impeded your productivity or efficiency?	RQ1, RQ3

Appendix B. Management Consent Form



Department of Information Systems

Leslie Commerce Building

Engineering Mall, Upper Campus

OR

Private Bag X3 - Rondebosch - 7701

Tel: +27 (0) 21 650 2261 Fax: +27 (0) 21650 2280

Internet: <http://www.commerce.uct.ac.za/informationssystemsl/>

August 2021

Request to conduct research and interview participation consent form

Dear Sir/Madam,

In terms of the requirements for completing a Masters Degree in Information Systems at the University of Cape Town, a research study is required.

The researcher, Grant Solomon, has chosen to conduct a research study entitled **“The Effects of Cultural Contradictions on Information Security Compliance Behaviour”**. The researcher would like to request permission to conduct this research study at your organisation.

The objective of the research is to explain how cultural contradictions influence information security compliance behaviour. The study is predicated on the idea that fostering a culture of information security, where compliance to security policies is second nature, is paramount to encouraging compliance behaviour. However, the security values of individuals or groups could differ from the organisation’s information security ideals. This study aims to understand how those differences are implicated in compliance behaviour. The outcome should give management insights into the human and cultural aspects of information security.

Participation in this research is voluntary and participants can choose to withdraw from the research at any time, in accordance with ethical research requirements. All information will be treated with utmost confidentiality and used exclusively for the purpose of this study. No individual or organisational identifiable information will be recorded or published, ensuring anonymity of responses.

The data will be collected using virtual interviews which will last approximately 30 to 45 minutes. If you authorise this study to be undertaken at your organisation, please kindly sign the attached form and return to me at your earliest convenience.

Should you have any questions regarding this research, please feel free to contact me on 0827728089 or email: slmgra002@myuct.ac.za

Your organisation’s voluntary participation in this study would be greatly appreciated.

Sincerely,

Signed by candidate

Grant Solomon

Researcher \ M.Com Student, (UCT)
Department of Information Systems
University of Cape Town
Email: slmgra002@myuct.ac.za

Supervisor

Prof. Irwin Brown

Research Supervisor
Department of Information Systems
University of Cape Town
Email: irwin.brown@uct.ac.za

Supervisor

Dr. Sharon Geeling

Research Supervisor
Department of Information Systems
University of Cape Town
Email: mlnsha001@myuct.ac.za

Management Consent

I, _____, give the researcher of this study consent to conduct their study in the following organisation:

I am aware that participation is voluntary and that participants may choose to withdraw from this study at any time, should they choose to do so.

Signature

Date

Appendix C. Individual Consent Form



Department of Information Systems

Leslie Commerce Building

Engineering Mall, Upper Campus

OR

Private Bag X3 - Rondebosch - 7701

Tel: +27 (0) 21 650 2261 Fax: +27 (0) 21650 2280

Internet: <http://www.commerce.uct.ac.za/informationssystem/>

August 2021

Request to conduct research and interview participation consent form

Dear Sir/Madam,

In terms of the requirements for completing a Masters Degree in Information Systems at the University of Cape Town, a research study is required.

The researcher, Grant Solomon, has chosen to conduct a research study entitled “**The Effects of Cultural Contradictions on Information Security Compliance Behaviour**”. The objective of the research is to explain how cultural contradictions influence information security compliance behaviour. The study is predicated on the idea that fostering a culture of information security, where compliance to security policies is second nature, is paramount to encouraging compliance behaviour. However, the security values of individuals or groups could differ from the organisation’s information security ideals. This study aims to understand how those differences are implicated in compliance behaviour. The outcome should give management insights into the human and cultural aspects of information security.

Your participation in this research is voluntary. All information will be treated with utmost confidentiality and used exclusively for the purpose of this study. No individual or organisational identifiable information will be recorded or published, ensuring anonymity of your responses. You can choose to withdraw from the research at any time for whatever reason, in accordance with ethical research requirements.

The data will be collected using virtual interviews which will last approximately 30 to 45 minutes. If you are willing to participate in this study, please kindly sign the attached form and return to me at your earliest convenience. Should you have any questions regarding this research, please feel free to contact me on 0827728089 or email: slmgra002@myuct.ac.za

Your participation in this study would be greatly appreciated.

Sincerely,

Signed by candidate

Grant Solomon

Researcher \ M.Com Student, (UCT)
Department of Information Systems
University of Cape Town
Email: slmgra002@myuct.ac.za

Supervisor

Prof. Irwin Brown

Research Supervisor
Department of Information Systems
University of Cape Town
Email: irwin.brown@uct.ac.za

Supervisor

Dr. Sharon Geeling

Research Supervisor
Department of Information Systems
University of Cape Town
Email: mlnsha001@myuct.ac.za

Research Participant Consent Form

I, _____, consent to participate in the research on

“The Effects of Cultural Contradictions on Information Security Compliance Behaviour”.

I am aware that participation is voluntary and that I may choose to withdraw from this study at any time, should I choose to do so.

Signature

Date

Appendix D. Ethics Approval Request



UNIVERSITY OF CAPE TOWN
FACULTY OF COMMERCE
Igniting Knowledge and Opportunity



Ethics Approval Request for the Study entitled:

The Effects of Cultural Contradictions on Information Security Compliance Behaviour

Signed by:

	Full name and signature	Date
Principal Researcher/Student:	Grant Solomon Signed by candidate	26/08/2021

This application is approved by:

Supervisor	Irwin Brown Signed by candidate	26-Aug-2021
Co- Supervisor	Sharon Geeling Signed by candidate	27/8/2021

Appendix E. Approved Ethics Application



Faculty of Commerce

Private Bag X3, Rondebosch, 7701
2.26 Leslie Commerce Building, Upper Campus
Tel: +27 (0) 21 650 4375/ 5748 Fax: +27 (0) 21 650 4369
E-mail: jacques.rousseau@uct.ac.za
Internet: www.uct.ac.za



@Commerce UCT



UCT Commerce Faculty Office

27 08 2021

Grant Solomon

Department of Information Systems

University of Cape Town

REF: REC 2021/08/026

The Effects of Cultural Contradictions on Information Security Compliance Behaviour

We are pleased to inform you that your ethics application has been approved. Unless otherwise specified this ethical clearance is valid until 31-Dec-2022 .

Your clearance may be renewed upon application.

Please be aware that you need to notify the Ethics Committee immediately should any aspect of your study regarding the engagement with participants as approved in this application, change. This may include aspects such as changes to the research design, questionnaires, or choice of participants.

The ongoing ethical conduct throughout the duration of the study remains the responsibility of the principal investigator.

We wish you well for your research.

Signed by candidate

2021.08.27
13:13:07 +02'00'

Jacques Rousseau

Commerce Research Ethics Chair

University of Cape Town

Commerce Faculty Office

Room 2.26 | Leslie Commerce Building

Office Telephone: +27 (0)21 650 2695 / 4375

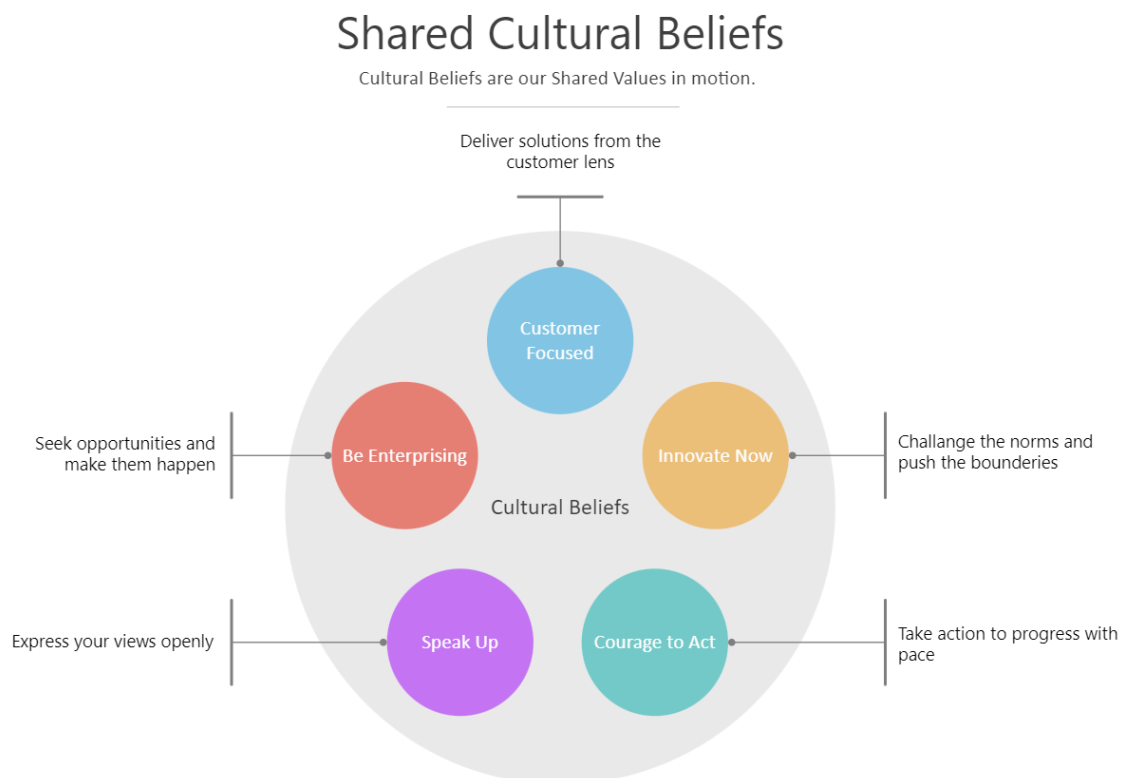
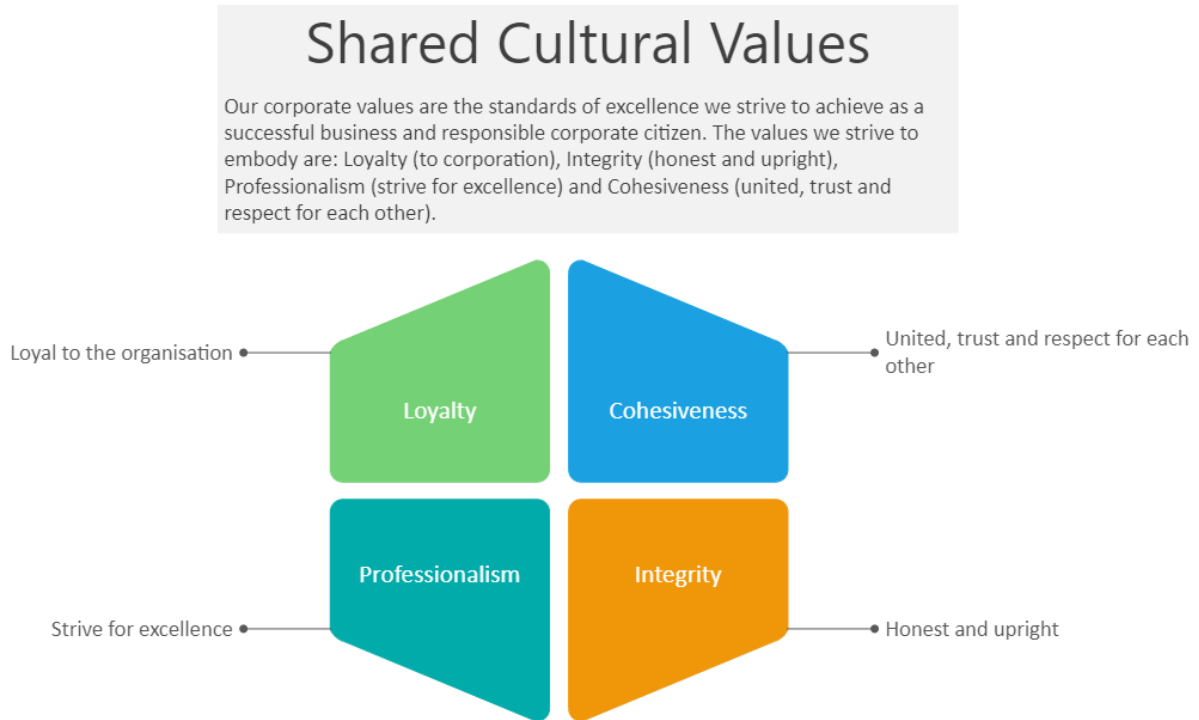
Office Fax: +27 (0)21 650 4369

E-mail: jacques.rousseau@uct.ac.za

Website: <http://www.commerce.uct.ac.za/com/Ethics-in-Research>

"Our Mission is to be an outstanding teaching and research university, educating for life and addressing the challenges facing our society."

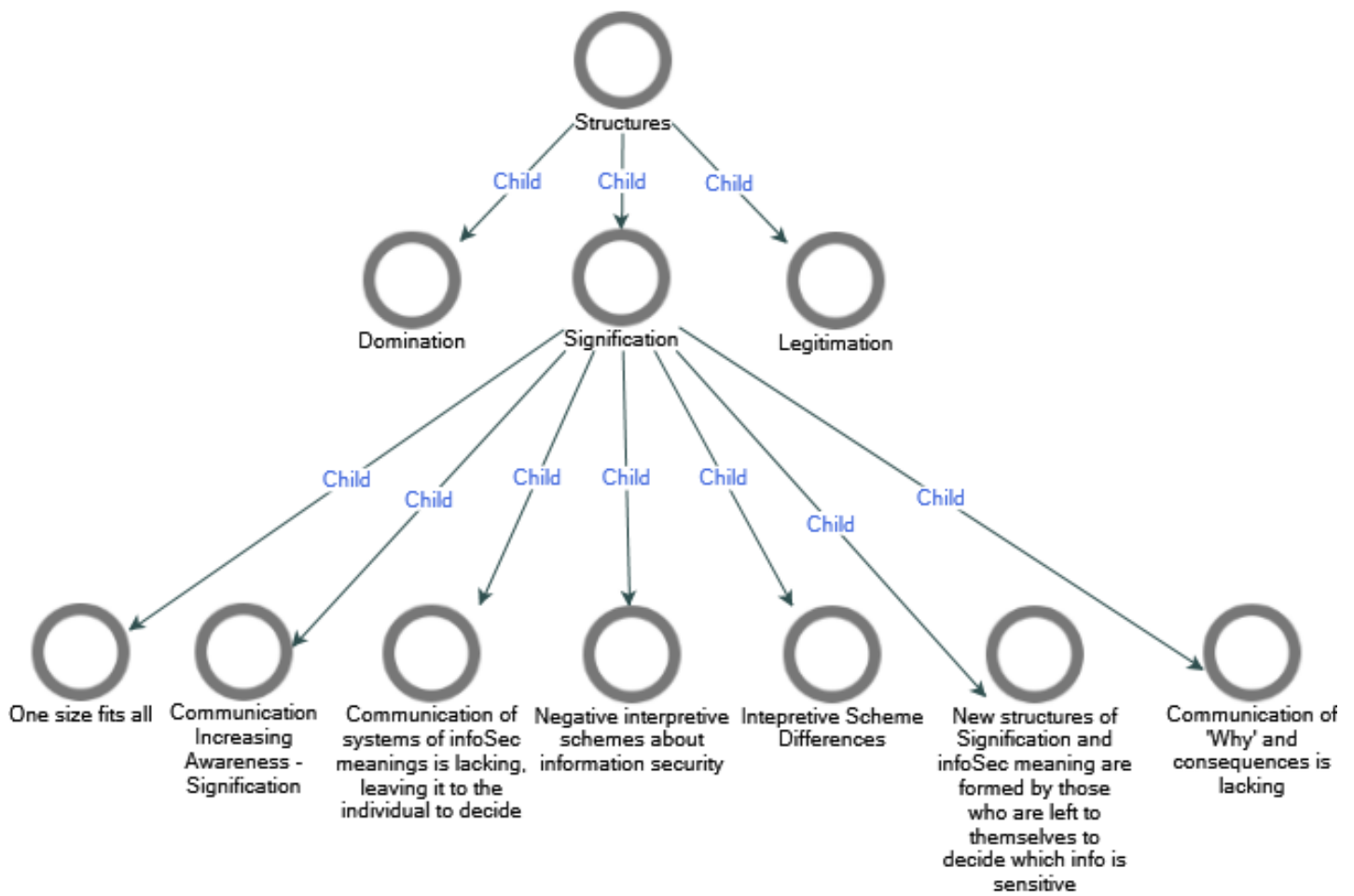
Appendix F. Sample Intranet Communication of Cultural Values

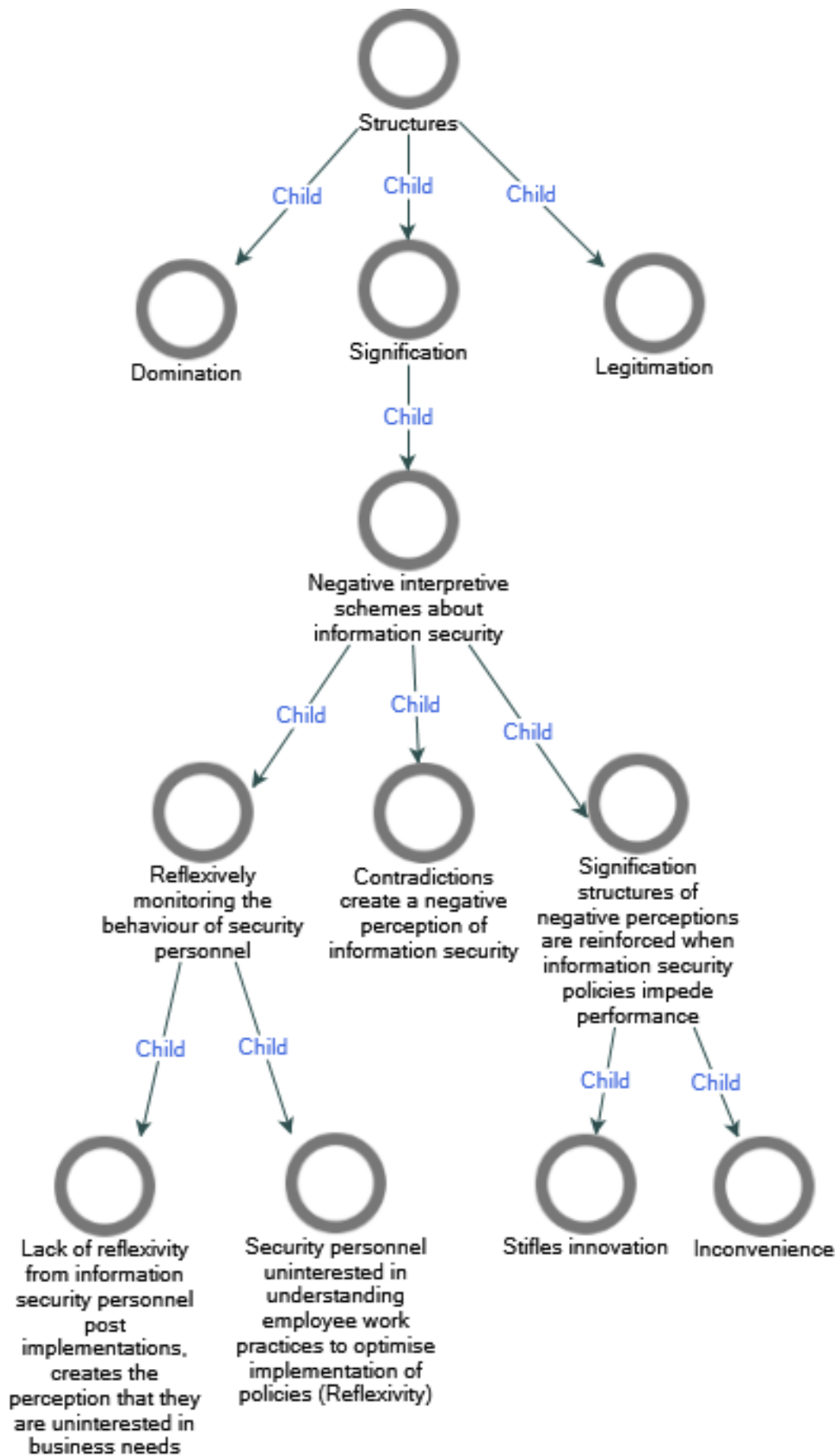


Cultural Beliefs Tools

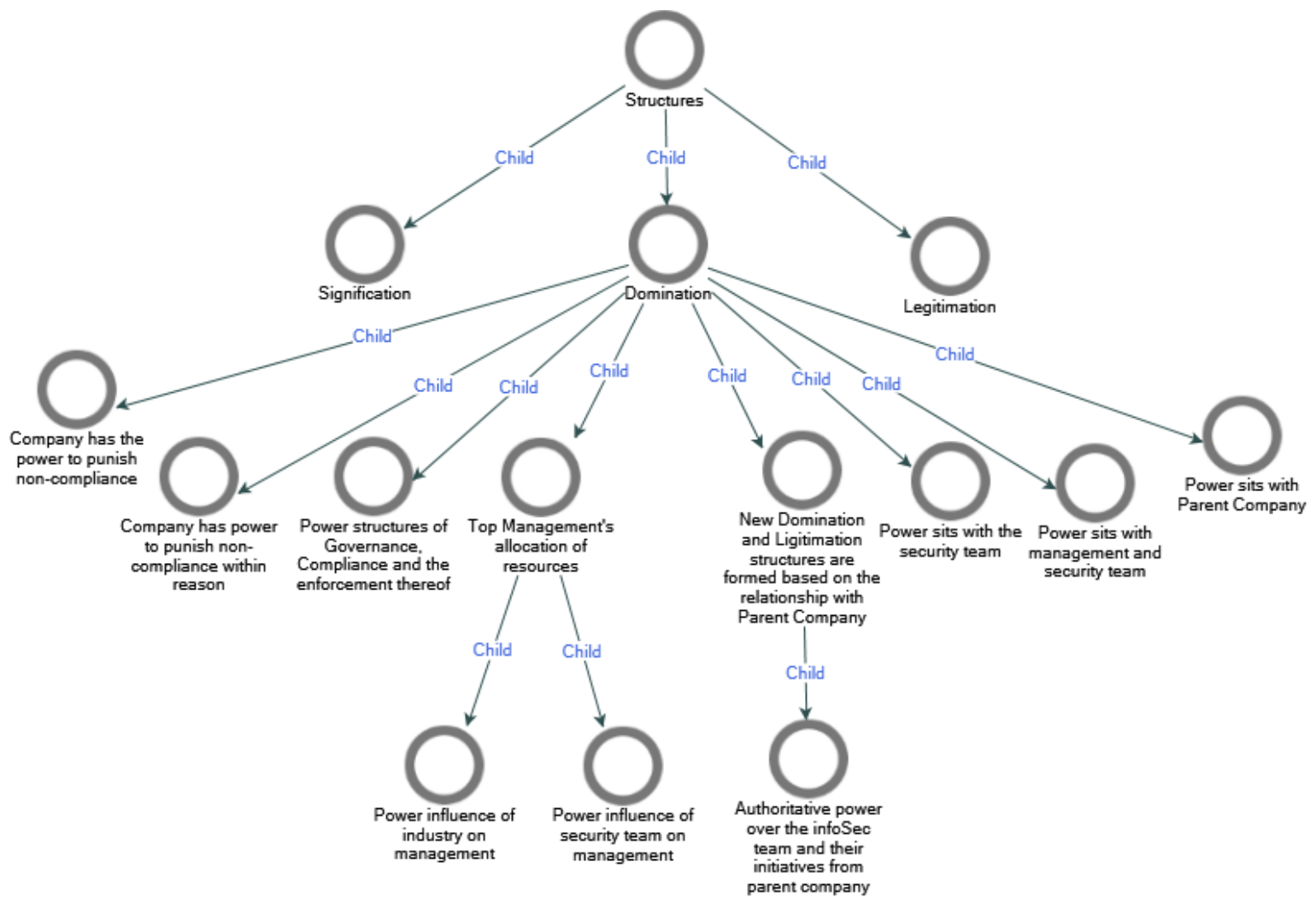
Focused Accountability	Focused Feedback	Focused Storytelling	Focused Recognition
A personal choice to rise above one's circumstances and demonstrate the ownership necessary for achieving Key Results	Feedback given around Key Results. Focused Feedback creates movement <i>in the right direction</i> .	Stories we purposefully and methodically tell about people and teams who demonstrate the Cultural Beliefs and impact R2 results.	Recognition focused around the Cultural Beliefs

Appendix G. Structures of Signification Themes





Appendix H. Structures of Domination Themes



Appendix I. Structures of Legitimation Themes

