Exploring the Moderating Effect of Organizational Culture on Employees Information Security Compliance

Dissertation submitted in fulfilment of the requirements for the Degree of Doctor of Philosophy in Information Systems

By: Kibrom Tadesse

Principal Supervisor: Prof.Mikko Siponen

Co-Supervisor: Dr.Tilahun Muluneh

Addis Ababa University

IT Doctoral Programme

Information Systems Track

February 2025

Addis Ababa University

School of Graduate Studies

IT Doctoral Program

This is to certify that the thesis prepared by, entitled: kibrom Tadesse ***Exploring the moderating effect of organizational culture on information security compliance in Ethiopia*** and submitted in fulfilment of the requirements for the Degree of Doctor of Philosophy in Information Systems complies with the regularities of the University and meets the accepted standards with respect to originality and quality.

Signed by Examining Committee:

External Examiner	**Signature**	**Date**
Prof.Gurpreet Dhillon.		
Internal Examiner	**Signature**	**Date**
Prof.Mikko Siponen		
Principal Supervisor	**Signature**	**Date**
Dr.Tilahun Muluneh		
Co-Supervisor	**Signature**	**Date**
Dr. Temtim Assefa		

Track Coordinator or Director of IT PhD Program

ABSTRACT

Employee non-compliance with Information Security Policies (ISPs) poses a significant and ongoing threat to organizational security, especially in developing countries like Ethiopia. Despite the implementation of formal policies and technical safeguards, organizations continue to experience insider threats resulting from behavioral non-compliance. This dissertation explores the factors that influence employees' intentions to comply with ISPs, focusing on how motivational drivers and organizational culture shape compliance intentions within specific organizational contexts.

Building upon Rational Choice Theory (RCT) and the Competing Values Framework (CVF), this study introduces an integrated model that investigates four motivational factors formal sanctions, perceived benefits, moral beliefs, and shame as predictors of compliance intentions. It also examines how these factors are moderated by four dimensions of organizational culture: consistency, cooperativeness, innovativeness, and effectiveness. By focusing on compliance intentions rather than actual behaviour, the study offers a more precise analysis of how motivational and cultural influences impact employee decisions, aligning with theory-driven approaches in organizational behaviour research.

The research employed a quantitative approach, surveying 553 employees from organizations across Ethiopia that had established ISPs. The collected data were analysed using Partial Least Squares Structural Equation Modeling (PLS-SEM) to test the hypothesized relationships and the moderating effects of organizational culture on compliance intentions.

The findings reveal that moral beliefs, formal sanctions, and perceived benefits are significant predictors of employees' intentions to comply with ISPs. More importantly, these relationships are strongly influenced by organizational culture. For instance, a culture of consistency amplifies the impact of both formal sanctions and moral beliefs on compliance intentions, while other cultural dimensions, such as cooperativeness and innovativeness, show more context-dependent effects.

This research makes several important theoretical contributions. It extends Rational Choice Theory by integrating organizational culture as a moderator, challenging the conventional view that compliance decisions are purely rational and individualistic. Additionally, it advances the Competing Values Framework by operationalizing its cultural dimensions at the individual level, a method seldom used in previous information security research. This approach addresses gaps in existing theories that overlook the intersection of motivational drivers and cultural contexts, particularly in non-Western, resource-constrained environments.

From a practical standpoint, the study provides valuable insights for policymakers and organizational leaders. It underscores the necessity of aligning formal compliance mechanisms with organizational culture, particularly cultural values that promote consistency and ethical behaviour. Such alignment can enhance the success of ISP implementation and reduce the risk of insider threats, offering a culturally grounded strategy for strengthening information security in developing nations.

Keywords: - *Information Security, Information Security Policy, Intention to comply with ISP, Insiders, Organizational Culture, Rational Choice Theory, and Computing Value Framework.*

ACKNOWLEDGEMENT

This PhD thesis is the outcome of a difficult journey that many people helped with and supported. I would like to honor some of them, if not all of them, at this time of accomplishment. First and foremost, I praise the Almighty God! I would like to thank everyone who has contributed their time and knowledge to the establishment of the incredibly successful PhD program at Addis Ababa University's IT-PhD office. For their invaluable contributions and support, I would like to sincerely thank Dr. Salehu Anteneh, Professor Solomon Negash, Dr. Temtim Assefa, Dr. Tibebe Beshah, and all of the track coordinators and office staff.

Professor Mikko Siponen

I appreciate your trust in me as your supervisee. Without your encouragement, support, and optimism, I could not have completed this thesis. He provided professional advice and helped me visit the University of Jyväskylä, Finland, to conduct extensive academic research and network with esteemed information systems researchers. Dear Professor, I will always remember you. I convey my appreciation for the help you provided.

Dr. Tilahun Muluneh

I am incredibly grateful for your help, and I owe you one. The challenges a PhD candidate faces come from both academic work and extracurricular activities, which can cause discouragement along the way. Your presence and support have been invaluable since our initial discussion about choosing a research title. You have been of great assistance to me. I'd like to thank you for encouraging me in my research endeavors and giving me faith in my academic abilities. I can't put into words how appreciative I am of you!

A special thanks to my family:

I would like to express my sincere gratitude to my lovely wife Martha Mulugeta and my kids (Barkon, Yafet, and Nolawi) for their unwavering support and encouragement. I am eternally grateful to my deceased father, Tadesse Ejigu, for providing me with the opportunities and experiences that have shaped my identity. You altruistically motivated me to place confidence in the significance of education and to engage in further exploration and acquisition of knowledge in one's existence. I express my gratitude to my mother, Silas Yeshak, for her support and assistance. I am fortunate to have sisters named Meskerem, Etalem, Nesanet, Kidist, Rahel,

and Liya. They not only serve as my siblings but also as my companions, and I am grateful for their constant support and encouragement in achieving my goals.

Many of you have contributed to my project's successful completion. Dr. Gashaw Kebede, Dr. Alemayehu Molla, and Dr. Abebe Rorissa have my sincere gratitude. You have endured the agony of reading this thesis word for word, and I have greatly profited from your insight. I am deeply indebted to you for your wonderful assistance and genuine concern. In addition, I want to thank Mohammed Abdulmenan and all of my friends for their encouragement and support as I worked towards my objective.

I am grateful to all of the personnel at the sample organizations who generously provided me with the data I needed for this research. I also want to thank everyone who answered the questionnaire. Your assistance was helpful. I also want to thank Wendwesen, Ziyine, Elsa, Kena and all the staff members of the sample organizations who assisted in gathering survey data. You made this task possible by helping me overcome data collection obstacles. I am incredibly grateful.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

1. AVE - Average Variance Extracted
2. AT - Agency Theory
3. CR - Composite Reliability
4. CVF - Computing Value Framework
5. GDT - General Deterrence Theory
6. HTMT - Heterotrait-Monotrait method
7. INSA - Information Network Security Agency
8. ISM - Information Security Management
9. ISP - Information Security Policy
10. IC - Internal Consistency
11. IT - Information Technology
12. NISP - National Information Security Policy
13. ISB - Information Security Behavior
14. OCAI - Organizational Culture Assessment Instrument
15. PMT - Protection Motivation Theory
16. PLS-SEM - Partial Least Squares Structural Equation Modelling
17. RCT - Rational Choice Theory
18. VIF - Variance Inflation Factor

DEDICATION

To my ever-supportive mother, Silas Yishak, whose unwavering belief in my academic journey has been a constant source of motivation, your pride in my pursuit of a PhD has fueled my determination, and today I am thrilled to share that I have achieved this milestone. This accomplishment is as much yours as it is mine.

Similarly, I wish to honor my beloved late father, Tadesse Ejigu, whose memory and encouragement have stayed with me despite his absence. With deep respect and affection, I dedicate this dissertation to him, knowing that he would have been proud of this achievement.

I extend my deepest gratitude to my loving wife, Martha Mulugeta, who has provided invaluable support throughout this challenging journey. I dedicate this work to my boys (Barkon, Yafet, and Nolawi), who make our lives happy, to inspire you and be a reminder that with dedication and discipline, you can achieve all you want.

DECLARATION

I, hereby, declare that the materials contained in this thesis have not been previously submitted for a degree at this or any other university. I further declare that this thesis is solely based on my own research. I also declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I understand that my thesis may be made electronically available to the general public for reference purpose.

Kibrom Tadesse

CHAPTER 1: INTRODUCTION

In today's information technology (IT) dominated world, information is a vital asset and an essential tool at the individual, organizational, societal, and national levels. Despite this fact, the failure of employees to comply with information security policy is a primary concern of information security scholars and practitioners in organizations. As technology continues to advance, many organizations face an increased number of security attacks on their systems (Alghazzawi et al., 2014). To address this reality, organizations funnel more and more resources to create a secure information system environment.

However, they only looked at the technical parts. These include hardware and software measures like firewalls, antivirus software, data backups, access controls, encryptions, and continuous monitoring that are built into a company's IT infrastructure (Ifinedo, 2012). They thought that most information security threats came from outside the company and that focusing on the technical parts would solve the problem (Crossler et al., 2013). In contrast to this, prior researchers have recommended that more threats occur due to internal factors (Walker-Roberts, S., Hammoudeh, M., & Dehghantanha, A., 2018). In their systematic review, they examined the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure (Walker-Roberts, S., Hammoudeh, M., & Dehghantanha, A., 2018).

Therefore, to properly understand the problem more deeply and tackle it, many researchers argue that the human aspect needs to be well addressed and studied. According to a report published in 2023, insider threats have increased by 47% from 2018 to 2022, costing an average of $13.75 million per year, globally. Various reports from multilateral organizations worldwide, such as Verizon, Kroll Annual Global Fraud and Risk Report, Haystax Technology, and the global information security survey by PwC, have also pointed out that insiders have become the most-cited culprits of information security breaches (Njowa et al., 2023).

For instance, according to the Securonix (2024) insider threat report, between 2019 and 2024, there was a notable rise in the prevalence of insider attacks, with the percentage of organizations reporting such incidents increasing from 66% to 76%. There has been a significant rise in concern for high-risk insiders, with the percentage increasing from 60% in 2019 to 74% in 2024.

This indicates a greater awareness or first-hand experience of intentional insider attacks (Securonix, 2024).

Although there have been attempts to safeguard vital infrastructure and improve training in cyber security, the main reason for incidents is still careless behavior, which accounts for 74% of all breaches (Verizon, June 2023). By observing the above reports, one can understand that human agents inside organizations are more dangerous than those outside organizations due to their access to data in their work activities and their intimate knowledge of the organizational information systems (Herath and Rao, 2009; M. Siponen and Vance, 2010).

In the context of low-income countries, Alfawaz (2011) claims that developing countries face information security breaches because there is very little knowledge about information security and management. Particularly in Africa, studies on information security are pretty minimal. The result of a study conducted by the Serianu cyber threat team in some African countries indicated that 50% of losses of all direct costs and 32% of overall costs are attributed to insider threats, which they estimate at USD 179,000,000 and USD 284,400,000 per annum, respectively (Team, 2022). The studies mentioned above clearly presented how insider threats pose a significant risk to their companies' information systems from a worldwide and African perspective.

When we observe the experience of Ethiopia, we witness the inadequacy of information security research (Arage et al., 2015). Furthermore, according to the Ethiopian News Agency (n.d.), *Prosperity Party's first-year performance reviewed* (https://www.ena.et/web/eng/w/en_10576), Ethiopia does not have a uniform and established legal framework, strategy, and governance for cyber security at the national level. Just 11.6% of government institutions in Ethiopia possess legal frameworks, which are currently in the trial stage. Most (87.4%) do not have established legal frameworks to prevent cyber-attacks (Adane, 2020). As a result, there is little recorded evidence that shows the possible occurrence and exact impact of information security threats in Ethiopia; therefore, it is hardly difficult to include statistics regarding non-financial as well as financial losses caused by insider threats.

Consequently, the present researcher made a preliminary assessment through interviews with randomly identified managers and IT security officers from commercial banks, universities, and other institutions. The data indicates that the institutions are experiencing security breach issues.

For instance, a bank clerk from the commercial bank of Ethiopia revealed that he had created a fake user account to withdraw and transfer 9.9 million Birr from various accounts using his access rights. He also revealed that he created fake user identifications to hack bank supervisors' passwords. In another instance of ISP violation, two bank employees withdrew funds from cash machines, misused access codes or passwords, or broke banking networks using stolen PIN numbers.

In another case, a bank clerk who went out for a toilet while his computer was logged in was cheated by his colleague, who transferred the money to another account (Hailu, 2015). In another instance, the noncompliance of an employee with the Ethiopian Customs Commission ISPs costs the customs commission 13,000,000 birr. In another incident, Ethiopian Airlines fired 11 staff because of noncompliance with the ISP procedures and rules they were supposed to comply with (Arage et al., 2015).

The studies outlined above clearly demonstrate that insider threats pose a significant risk to organizations' information systems worldwide. Moreover, these threats are prevalent in Ethiopia, highlighting the urgent need for research in this area. It is crucial to consider the role of organizational culture in shaping employee behavior, as it plays a central role in influencing attitudes toward security policies and practices. Organizational culture comprises shared values, beliefs, standards, and behavioral norms that guide and constrain behavior within the organization (Schein, 2004). Thomson et al. (2006) argue that understanding the relationship between organizational culture and employee behavior is critical, especially in the context of information security. Corporate culture can significantly affect how employees perceive and comply with information security policies, either fostering adherence or enabling noncompliance (Lim et al., 2009).

Numerous scholars (Butler & Brown, 2023; D'Arcy & Greene, 2014; Vance et al., 2020) have underscored that organizational culture plays a critical role in determining the level of compliance with information security policies. The organizational culture within a company can either facilitate or hinder the adoption of security measures, influencing how employees engage with security protocols. Despite the importance of organizational culture in shaping behavior, Karlsson et al. (2015) noted that there is still a lack of research on the specific effects of

organizational culture in the context of information security compliance. This gap has been further confirmed by our review, which suggests that existing research offers limited practical guidance for addressing the challenges posed by organizational cultures in fostering ISP compliance.

The prevailing theories on information security compliance, such as General Deterrence Theory (GDT) and Protection Motivation Theory (PMT), predominantly focus on fear-based approaches and offer limited insights into how organizational culture influences employee behavior (Vance & Siponen, 2012). In contrast, the Rational Choice Theory (RCT), which this study adopts, considers a wider range of factors, such as expected benefits and moral beliefs, thus offering a more holistic perspective on information security compliance (Li et al., 2010). Furthermore, much of the empirical research on ISP compliance has been conducted in developed countries, leaving the distinct dynamics of developing nations largely unexplored (Cram et al., 2019; Tilahun & Tibebe, 2017). This highlights the need for research that considers the impact of organizational culture on ISP compliance in diverse cultural contexts. Moreover, it would not be difficult to incorporate additional statistics related to the financial and non-financial losses caused by insider threats (Adane, 2020). These losses often stem not only from technical vulnerabilities but also from deeper organizational issues. In line with this gap, it is therefore essential to assess the potential occurrence of information security breaches while also considering the role that organizational culture plays in either mitigating or exacerbating such threats.

1.1 Statement of the Problem and Research Questions

Information security breaches continue to pose significant threats to organizations globally, compromising sensitive data, undermining trust, and incurring substantial financial losses (Greene, Gwen, & D'Arcy, 2010; Sohrabi Safa et al., 2016). The research (Ophoff et al., 2014) highlights that insider’s pose a significant risk to information security. Despite extensive research efforts, the persistent failure of employees to adhere to information security policies and procedures remains a pressing concern (Ophoff et al., 2014), several gaps remain.

Despite the existence of past work, many empirical studies that are conducted to investigate individuals' information security compliance are mainly focused on fear-based strategies and

provide only partial insight (Vance et al., 2012). Furthermore, most of the existing work has focused on either awareness, a training approach, or systemic design to mitigate information security policy breaches. Moreover, the existing information security compliance studies have looked very minimally at the role played by organizational culture in enhancing information security compliance (Ifinedo, 2014); Safa, et al., 2016; AlKalbani, et al., 2017).

Furthermore, the majority of existing research originates from developed regions like Europe and North America, neglecting the unique cultural and contextual factors that characterize organizations in developing nations, particularly in Africa (Arage et al., 2015; Vance et al., 2020). This gap is particularly pronounced in Ethiopia, where information security challenges persist, yet research on non-technical solutions remains scarce (Adane, 2020; Desisa and Beshah, 2014; Tilahun and Tibebe, 2017; Woretaw and Lessa, 2012).

This study, therefore, sought to address these missing links by investigating the moderating role of organizational culture in shaping employees' intentions to comply with information security policies in Ethiopian organizations. By adopting a multi-dimensional approach that integrates insights from rational choice theory and the competing values framework, this research seeks to provide a comprehensive understanding of the complex interplay between individual beliefs, organizational culture, and compliance behavior. The study aimed to provide the validation component of the emerging theoretical model based on results grounded in empirical quantitative data.

In today's information-driven environment, organizations face significant risks associated with information security breaches, which can result in severe financial losses, compromised data integrity, and diminished organizational trust. Although many organizations worldwide have invested in technical safeguards such as firewalls, encryption, and intrusion detection systems, these measures alone have proven insufficient to address security breaches stemming from internal actors employees and contractors who, knowingly or unknowingly, compromise information security policies (ISP). This issue is especially pronounced in developing regions, including Ethiopia, where information security practices and policies are still evolving, and non-

technical, human-centered aspects of compliance are often overlooked (Adane, 2020; Desisa and Beshah, 2014; Tilahun and Tibebe, 2017; Woretaw and Lessa, 2012).

Research indicates that in Ethiopia, organizational compliance with ISPs faces unique challenges. The absence of standardized regulatory frameworks, resource constraints, and limited information security awareness create conditions that allow insider threats to thrive. Furthermore, the Ethiopian organizational context has distinct cultural and operational norms that may affect compliance behaviors differently than in Western contexts where most studies have been conducted. Insider threats are particularly critical, as employees' privileged access to sensitive information and organizational systems positions them to inadvertently or maliciously violate ISPs. Consequently, understanding how organizational culture influences compliance intentions in Ethiopian organizations is crucial for developing effective, context-specific solutions.

While considerable research has explored information security compliance, most studies have focused on fear-based, deterrent strategies or technical solutions. These approaches, however, overlook the influence of organizational culture on compliance behavior, particularly within the context of developing countries. Limited studies, especially in Ethiopia, have examined the impact of organizational culture as a moderating factor in employees' intentions to comply with ISPs. Additionally, frameworks such as Rational Choice Theory (RCT) and the Competing Values Framework (CVF) — though used extensively in management and security compliance studies — have yet to be fully applied to analyze how cultural dimensions like consistency, cooperativeness, and flexibility influence compliance intentions. Given the diverse motivations that drive employee behavior, such as perceived benefits and moral beliefs, a multi-dimensional framework that includes both individual and organizational factors is necessary.

This study seeks to address these gaps by investigating how specific dimensions of organizational culture moderate the influence of formal sanctions, informal controls, perceived benefits, moral beliefs, and shame on employees' intentions to comply with ISPs within Ethiopian organizations. By integrating RCT, which considers both economic and moral motivations, and CVF, which categorizes organizational culture into quadrants that emphasize values like cooperativeness and consistency, this research will contribute to a more nuanced

understanding of compliance behavior. Specifically, this study will test the hypothesis that organizational culture dimensions such as consistency and cooperativeness strengthen or weaken the effects of formal sanctions and personal beliefs on compliance intentions.

Research Questions

RQ1: What is the influence of informal sanctions, formal sanctions perceived benefits, moral beliefs, and shame affect employees' intentions to comply with their organization's ISPs?

RQ2: What is the moderating impact of organizational culture on the relationship between formal sanctions, perceived benefits, moral beliefs, and shame, and employees' intentions to comply with their organization's ISP?

1.2 Objective

The following objectives, classified as general and specific, are set out to address the research question. The specific objectives are designed to fulfill the overarching objective stated below.

1.2.1 General Objective

The general objective of this research is to develop and test an empirical model that demonstrates the moderating influence of organizational culture on the impact of formal sanctions, perceived benefits, moral beliefs, and shame on employees' intention to comply with ISPs.

1.2.2 Specific Objectives

To achieve the general objective of the study, we accomplished the following specific objectives:

- Identify, present, and discuss the various dimensions of the organizational cultural model.
- Identify, present, and discuss the different dimensions of rational choice theory.
- Test the moderating effect of the dimensions of organizational culture in a survey study among employees who work in organizations located in Ethiopia.
- Identify and discuss the critical organizational cultural factors to consider when developing and implementing organizational ISPs and practices.

- Identify and discuss the essential RCT factors to take into account in the process of developing and implementing organizational ISPs and practices.
- Develop an empirical model that tests the moderating effect of organizational culture dimensions between RCT constructs and employees' intentions to comply with ISPs.
- Provide recommendations for future researchers in the field of information security who need to investigate ISP practices among organizations.

1.3 Overview of the research model and hypotheses

To achieve the objective and answer the research questions, the correct conceptual model must be formed. The research model was developed by combining CVF and RCT, as shown in Figure 2. 1 . The following sections will present explanations of how we constructed the current study's theoretical framework and the theories we selected, drawing on several previous pieces of literature.

1.3.1 Relational Choice Theory.

A growing body of research has addressed humans' information security behavior, and several theories have been applied, to mention some: D'Arcy et al. (2009) used general deterrence Theory (GDT),and Bhatti et al. (2021) used Agency Theory (AT). Herath and Rao (2009) used Protection Motivation Theory (PMT). Pahnila et al. (2007) combine the protection motivation theory, and the general deterrence theory. Li et al. (2010) assert that GDT and PMT are the two major theories dominating information security compliance studies. However, many empirical studies conducted to investigate individuals' information security behavior (ISB) have mainly focused on fear-based strategies, providing only partial insight (Vance et al., 2012). In contrast, this study adopts a broader perspective by examining the influence of organizational culture factors on ISP. By doing so, it aims to provide a more comprehensive understanding of what drives secure behavior within organizations beyond just fear appeals.

Therefore, we choose to use a theory that can excel in this scope to obtain a good understanding and answer the question, "How can we enhance or achieve ISP compliance in organizations?" In

this context, rational choice theory exceeds this limitation because it includes additional constructs like moral beliefs and perceived benefits.

Based on Rational Choice Theory (RCT), not all individual choices are economically driven; other factors, such as perceived benefits and personal values, may also influence decision-making. Hence, we conclude that RCT encompasses all sorts of benefits; it focuses not only on perceived economic benefits an individual might get by violating the regulations and the rules (Ifinedo, 2016). We also agree with what Bukaty (2012) said; McCumber (2011) has oversimplified rationality.

Vance and Siponen (2012) assert that "individuals will always undergo a useful calculation when they make decisions about violating or complying with rules." Furthermore, the impact of RCT's constructs, such as shame, on employees' ISP compliance has received minimal investigation, with the exception of Vance and Siponen's (2010) study. Despite this relevance, there is a lack of research applying RCT constructs in African organizational contexts. For example, Tilahun & Tibebe (2017) did not investigate any RCT-related factors. This study therefore not only applies a theoretically sound model, but also addresses a contextual research gap.

1.3. 2 Competing Values Framework Theory

According to Leidner and Kayworth (2014) definition of organizational culture, "represent a manifestation of a culture that signifies espoused beliefs identifying what is important to a particular cultural group." Similarly, Tsui et al. (2006) define organizational culture as "a set of core values consensually shared by organizational members."

This definition recognizes the value of culture. Thus, this present study follows the value perspective of culture to explore its role in an organizational context quantitatively. This study followed several studies of organizational culture.

It implemented the CVF of organizational culture to operationalize these shared values and beliefs that represent the underlying organizational culture. The value-based Quinn (2011) model has been heavily changed and used in quantitative studies of organizational culture. It has been a useful tool for testing the link between organizational and individual cultural values and behavior (Iivari and Huisman, 2007; Jones et al., 2005).

As pointed out by Cameron and Quinn (2005), there are numerous frameworks or models available in the studies about organizational culture, to mention some: Tsui et al. (2006) five dimension model, Hofstede et al. (2010) six dimension model, and many others. Though the functionality of the main model remains unchanged, the framework of Quinn (2011) has changed over the years, with distinct labels for the four cultural meanings.

This research adopts the Ernest Chang (2007) CVF model, developed by K. Cameron and Sine (1999), because it provides a comprehensive yet parsimonious framework for understanding organizational culture. The model integrates key elements of the Competing Values Framework (CVF), which captures the complexities of organizational culture through dimensions such as flexibility vs. control and internal vs. external focus. This integration is particularly well-suited for examining the dynamics of organizational culture in our study, as it offers both theoretical depth and practical applicability to explore cultural alignment in the context of ISP.

This organizational culture has two dimensions: one reflects the extent to which an organization has a control or flexibility orientation, and the other reflects the extent to which it is focused on its own internal or external functions. These two dimensions form four quadrants cooperativeness, innovativeness, consistency, and effectiveness, representing distinct organizational cultures.

In conclusion, we primarily selected constructs from the RCT and CVF theories, concentrating on variables predicted to significantly influence employees' compliance behavior. In addition to this, we include variables that have been reported to have an inconsistent impact on employees' compliance behavior so that our study sheds light on the factor that might contribute to the inconsistent finding. The hypotheses proposed in this study are presented in chapter 2.

1.4 Significance of the research

In general, this research is significant as it addresses the critical issue of information security, highlights the importance of the human aspect of information security, fills the research gap in Africa, and investigates the impact of organizational culture on ISP compliance in Ethiopia. In detail, the significance of this study can be summarized as follows:

While organizations focus primarily on technical measures to protect their systems, research indicates that the human aspect of information security, including employees' behavior, is equally critical to mitigating security risks. Insider threats, where employees with privileged access to organizational data and information systems pose a significant risk, are increasing, and studies suggest that human agents inside organizations are more dangerous than those outside organizations.

There is a lack of studies worldwide, especially in Africa, that examine non-technical factors such as organizational culture that influence employees' intention to comply with information security policies. Although information security issues are evident in Africa, particularly in Ethiopia, there is hardly any research that considers non-technical solutions to this problem.

Organizational culture is one of the non-technical factors that influence human behavior and is gaining increasing interest in this area. However, research on the impact of organizational culture on ISP compliance is scarce, especially in developing nations. Therefore, this research aims to fill this gap by examining how organizational culture moderates the impact of formal sanctions, informal sanctions, perceived benefits, moral beliefs, and shame on employees' intention to comply with ISPs in Ethiopia.

1.5 Scope of the Study:

This study focuses on organizational culture (OC) at the individual level within organizations. While it is recognized that employee behavior is shaped by various factors (such as leadership styles, external influences, individual characteristics, and organizational structure), the study places emphasis on organizational culture because of its central role in shaping employees' values, behaviors, and decision-making processes. Organizational culture has a significant influence on employee behavior, as it dictates shared values, norms, and practices that guide how employees interact with each other and with organizational goals. By focusing on OC, the study aims to explore how cultural types (i.e., cooperativeness, innovativeness, consistency, and effectiveness) influence behavior, particularly in relation to Rational Choice Theory (RCT) constructs.

It is acknowledged that other factors can also influence employee behavior. However, this study specifically focuses on organizational culture because of its unique and pervasive influence on

organizational dynamics. The current focus on OC allows for a more focused investigation of the cultural dimensions that directly affect employee decision-making in the context of information security behavior. This study's scope is intentionally limited to organizational culture to maintain clarity and depth in addressing the research questions.

Regarding the Competing Values Framework (CVF), the study focuses on the vertical dimension of the model, which differentiates between organizations with a flexibility orientation and those with a control orientation. The vertical dimension of the CVF is particularly relevant because it provides insight into how the organization's overall approach to flexibility and control influences individual behavior, decision-making, and compliance with organizational norms and policies. By focusing on this dimension, the study explores how organizational culture's orientation toward flexibility or control impacts employee behavior in the context of ISP. Including all dimensions of the CVF might have introduced unnecessary complexity and could have diluted the focus on the most pertinent aspect of organizational culture for this study. Therefore, limiting the scope to the vertical dimension ensures a more targeted and manageable analysis.

1.6 Organization of the Thesis

The thesis is structured according to the guidelines of the Graduate School of Addis Ababa, using the monograph approach. This includes an introduction, literature review, method, analysis, and results, as well as a discussion, recommendation, and conclusion chapter. The introduction provides background information, research gaps, problem statements, objectives, and the significance of the research. The literature review discusses previous academic works in the area and explains the research model and hypotheses. The method chapter explains the research paradigm, strategy, and data collection technique. The analysis and results chapter describes the sample, method bias detection and control, descriptive statistics, measurement model evaluation, and structural path analysis. The discussion, recommendation, and conclusion chapter summarizes the findings, compares them to previous works, explains the contributions, highlights limitations, makes recommendations for future research, and evaluates the overall contribution of the research.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This chapter presents an overview of the key concepts that are essential for the research. It provides a brief review of the existing literature on "information security and insiders" and "information security policy." As these concepts are fundamental to this study, this section focuses on explicating the various aspects of these terms that are related to "behavioral factors and information security policy, ISP compliance," and "related works," and "culture."

Given the significance of these concepts in the study, this section specifically focuses on explaining the different aspects of these terms related to "organizational culture, dimensions of organizational culture, measuring organizational culture, employee behavior, and organizational culture ". Based on the previous works' review, the chapter highlights the central concept for the study of organizational culture and information security and examines organizational culture, employee behavior, and information security to provide a comprehensive understanding of the phenomenon.

Subsequently, the following section provides an integrative review of the most relevant theoretical frameworks used in this study to establish the knowledge context. The constructs drawn from RCT and CVF theories will be discussed based on the specific theories selected as a dominant framework for this study. This discussion will explain the research model's development and the corresponding hypotheses.

2.2 Information Security and Insider Threats

Organizations possess various assets, with information being one of the most valuable. It is an essential resource that allows companies to achieve their objectives. However, if information falls into the wrong hands, it can have a detrimental impact on the company's continuity, lead to financial losses, and damage the organization's reputation. Therefore, information must be protected from all types of attacks. Nevertheless, the growing dependence of organizations on information and communication technology is constantly increasing their concerns about information security (Susanto and Almunawar, 2018).

Information security has become a core issue for every organization. Its objective is to safeguard sensitive information and information systems from unauthorized access, disclosure, modification, disruption, and destruction. Adequate controls must be implemented to protect information resources, align with the organization's security objectives, and minimize risks. However, information security is vulnerable to several types of threats, including natural threats, physical security threats, and human threats. Natural threats include natural disasters such as earthquakes, hurricanes, and floods, among others. Physical threats include resource loss or damage caused by fire, water, theft, or physical impact. Human threats include attacks carried out by both insiders and outsiders. Outsider attacks are carried out by individuals who are not affiliated with the organization.

In information security behavioral studies, an "insider" generally refers to users who have access to the organizational information systems and knowledge of the institutional processes, enabling a wide variety of information security breaches, including destructive, unethical, or illegal (Browne, 2018). In this research, an insider refers to former or current employees or contractors who have authorized access to the organization's information, techniques, technology, and information assets.

The insider threat coordination center defines an "insider threat" as "the ability for a person who has or had authorized access to an organization's resources to exploit their access, either maliciously or unwittingly, to do harm to the organization" (Costa, 2017). The updated definition incorporates both malicious and accidental insiders, replacing the initial meanings that were distinct and unique. Therefore, the new definition is generalized, addressing insider threats as individuals with or with privileged access and acting "in a manner that may have an impact on the organization, either in a malicious way or unintentional." This study uses a definition that combines both malicious and unintentional insider threats.

When comparing internal with external threats and assessing an organization's vulnerability and the possible harm incurred by an insider, it is helpful to consider previous studies or reports. Insider threats continue to be a problem for organizations of all sizes and industries (Alsolami, 2015; Theis et al., 2019). According to the Securonix insider threat 2024 finding, from 2019 to

2024, the number of organizations reporting insider attacks increased from 66% of organizations to 76%, indicating a substantial increase in detected insider threats (Securonix, 2024).

The 2023 insider threat report presents several significant findings. Approximately three-quarters of organizations report that insider attacks have increased in frequency. Additionally, around 74% of organizations acknowledge that they are at least moderately susceptible, or even more so, to insider threats. Over 50% of organizations have encountered an insider threat within the past year, with 8% experiencing more than 20 incidents. A significant majority of respondents, accounting for 68%, express a level of concern ranging from moderate to high regarding insider risk as their organizations make the transition back to the office or adopt a hybrid work model (Raja, 2023).

Moreover, the Ponemon institute 2023 insider threats global report interviewed 1,075 IT and IT security practitioners in 309 organizations across North America (the USA and Canada), the Middle East, Europe, Asia Pacific and Africa. They mentioned they experienced one or more material events caused by an insider. A total of 7,343 insider incidents are represented in this research. The report also revealed that there was an increase in insider threat incidents from 2020 to 2022 (Mosqueda, 2023). According to the 2022 cost of insider threats global report, companies experience an average annual cost of $15.4 million due to insider threat incidents (Mosqueda, 2023). Insider threats can affect all aspects of information security in an organization and often occur without warning or risk.

Two notable cases of insider threats are Edward Snowden and Anthony Levandowski. Edward Snowden, an information technology contractor, obtained critical information from the national security agency without sharing his passwords with colleagues, revealing that it's easy to access sensitive data. In 2013, Snowden's actions put insider threats on the media's agenda. Because insiders have approved access privileges, it's challenging to distinguish between legitimate uses and malicious attacks, as noted by Tripwire in 2017. Anthony Levandowski was accused of stealing 14,000 files from Waymo, google's former self-driving car division, and bringing them to Uber, his new employer. Levandowski established a company, which Uber acquired for $680 million after stealing Waymo's intellectual property.

The literature and reviews in the field of information security consistently highlight the internal threat as the most significant challenge for organizations. Security specialists widely believe that insider attacks are more costly and effective than external threats. For example in the 2023 insider threat report, 48% of respondents concur that insider attacks pose a greater challenge in terms of detection and prevention compared to external attacks. Identifying insider threats can be difficult because these threats utilize authentic accounts and credentials while exploiting information technology tools, making it challenging to distinguish them from regular user activity. These findings imply that security teams should allocate significant resources to protect against these threats in the upcoming years (Raja, 2023). Studies show that insiders are the primary source of security violations in companies, despite the availability of modern definition of technology and surveillance protocols (Hu et al., 2012).

Thus, insiders remain the greatest threat to information systems. However, obtaining well-documented information or published research on information security, especially on insider attacks in Ethiopian institutions, is challenging (Adane, 2020; Desisa and Beshah, 2014; Tilahun and Tibebe, 2017; Woretaw and Lessa, 2012). In a preliminary analysis we have done, we found some evidence of insider attacks in Ethiopian institutions, similar to Arega's findings. We also summarize studies that highlight the information security issues in Ethiopian institutions.

The first national information security policy (NISP) of 2011 addressed Ethiopia's vulnerability in detail and recommended developing an NISP to minimize threats and vulnerabilities. The policy also emphasized the importance of integrating organizational security with national security. The 2022/2023 annual report of the Information Network Security Administration (Harvey et al.), indicated the existence of external and internal challenges. A recent study on the information security of Ethiopia's financial sectors found that the level of protection and governance culture regarding information security is not good enough. To improve information protection in Ethiopia's banking sector, efforts must be made across all areas and with a plan (Shimels and Lessa, 2023; Yohannes et al., 2019).

Local studies examine various topics, Ejerssa (2018) study found that information security implementation in Ethiopian public universities did not meet the standard. Yemane (2018) findings indicated that Ethio Telecom’s information security management practices did not fully

comply with ISM practices and met a low international standardization organization standard level. This highlights the need for improvements in information security practices within the organization. (Abebe and Lessa, 2020) interview analysis uncovered the employees' culture, awareness, and comprehension, as well as the imperative to safeguard the banks' information. Nevertheless, they seemed to disregard the information systems security policy and procedures necessary to ensure information systems security.

The findings indicate that the insecure behavior of the information systems can be attributed to the lack of effectiveness in the banks' information systems security training. Yohannes et al. (2019) conducted a qualitative case study to assess bank practices regarding information security incident management and found that banks did not have a predefined plan for information security incident management. Getaneh (2018) study revealed that critical Ethiopian organizations were not adequately prepared to detect, prevent, and respond to cyber threats and violations. Abebe and Lessa (2020) study also showed that user behavior could put the banking system at risk. Getnet (2020) found general gaps in information systems security management practices in Ethiopian organizations, such as a lack of experienced human resources, policy, training, and understanding of non-compliance with rules and regulations. According to a survey conducted by the Ethiopian computer emergency response team in 2019, internal workers were responsible for the majority (52.6%) of information security incidents reported in the country.

Most studies on Ethiopian information security issues recommend technological solutions, but such solutions alone cannot provide the required security level. Behavioral issues, such as organizational culture, receive little attention in information security research (Tilahun and Tibebe, 2017; Tsakumis et al., 2007).

2.3 Information Security Policy

In the business world today, the organizational process involves improving efficiency and minimizing running costs. One way to achieve this benefit is to use IT applications or information systems to advance company processes and boost transactions (Chaâri et al., 2016; Clemons et al., 2017). When a company incorporates new technologies, it must also ensure that security policies are implemented for employees to understand management expectations when using new information systems securely (Sommestad et al., 2015). Implementing an information

security policy is one way for businesses to counter the threat of information technology, reduce possible theft, and prevent sensitive company knowledge leaks (Idahosa, 2020; Trim and Lee, 2019).

An information security policy is a document or set of documents describing the company's high-level security controls to protect its information from internal and external attacks (Antoniou, 2015; Flowerday and Tuyikeze, 2016). It describes an organization's entire security architecture, including clear objectives, rules, and regulations, and formal procedures. These policies serve as the foundation for the security infrastructure (Antoniou, 2015).

They secure and protect an organization's information resources while also providing legal protection. Security policies encourage employees to collaborate to ensure organizational communication and reduce the risks of security awareness caused by human factor errors such as disclosing sensitive information to unauthorized or unknown sources or better use of the internet. They also protect against cyber-attacks, malicious threats, foreign intelligence, and other potential threats. The main topics covered are physical security, network security, access authorization, virus protection, and disaster recovery. All policies must be backed up by adequate safety standards, procedures, and guidelines (Antoniou, 2015; Cram et al., 2017).

The overall goal of the information security policy is to create a more secure environment. Individual obligations should be defined in a robust security strategy, as should punishments for breaches and a process for upgrading the policy (Peltier, 2016). The ISP is critical in demonstrating management's dedication to and support for information security. While the information security policy provides a framework for facilitating security violation prevention, detection, and response, the policy document is typically backed up by standards that are more technical or operational. In recent years, scholarly and specialist groups have agreed that the formulation and implementation of an effective ISP are essential to the security of organizational information systems. As described in the Peltier (2016) study, the information security policy is already a requirement for successful security management. Without it, the company could face a slew of information security issues.

Although the ISP can play an essential role in practical information security management, there is growing recognition that the policy is unlikely to be a successful security tool unless

organizations follow a number of key prescriptions in policy implementation (Antoniou, 2015; Cram et al., 2017; Peltier, 2016). For example, the policy must be widely and strongly disseminated within the organization, and employees must be informed of the guidelines that protect company information and assets through security policies. A well-written policy will outline acceptable and prohibited uses, reducing risks automatically if employees follow the guidelines. Security policies also provide a solid foundation for conducting network and resource audits. They serve as a starting point for finding vulnerabilities and conducting forensic activities if security has been compromised (Peltier, 2016).

2.4 Information Security Behavior and Information Security Policy

While the use of information security has brought many benefits to organizations, handling knowledge with information security also poses risks. Cybercriminals who infiltrate an organization's systems are significant threats, and organizational staff not following its ISP can also lead to security breaches. More than half of information security violations are estimated to be due to insufficient compliance by employees with ISPs (e.g., Dhillon & Moores, 2001). Therefore, it is essential to understand why ISB can affect compliance with ISPs.

Four critical topics for future information safety research were identified by (Crossler et al., 2013). Firstly, understanding and differentiating between misbehavior and supervision of insiders. Secondly, defining and determining hackers' motivations. Thirdly, improving compliance with information security by determining which incentives and dangers are useful motivators for differing factors. Fourthly, user information security management is one of the most critical points in today's workplace. All these suggestions are related to employees’ or individuals' behavior. This behavior has been identified as the greatest threat to an organization's information security (Puhakainen, 2006), and the inability of employees to follow ISP policies is estimated to account for over half of all violations of information security in organizations.

ISB can take several forms and be motivated by various intentions, as demonstrated by Stanton et al. (2005) categories. ISB is considered to be affected by a variety of social, individual, and business considerations. These factors can be defined as the user's perception of what is required of them in terms of information security and their ability to behave in compliance with these expectations (Abraham, 2011). The principles, strategies, and culture of the organization, the

attitudes of managers and colleagues, and users' common knowledge of information security problems and decision-making capabilities all affect how ISPs are perceived. ISB, on the other hand, is influenced by individuals' values and standards, their psychological contract with their employers, and the effort required for compliance (Abraham, 2011). Various ISB models have identified these and a slew of other variables, and two of the more widely used models are presented below.

ISB has been described by various theoretical models, two of which are frequently used: deterrence theory and protection motivation theory. DT focuses on the importance of formal and informal sanctions, and PMT presents a threat and coping appraisals as techniques for determining behavior. Empirical experiments demonstrating ISB have produced mixed findings (e.g., Cheng, Li, Li, Holm, & Chai, 2013; Herath & Rao, 2009a; Li, Zhang, & Sarathy, 2010) (e.g., Kim, Yang, and Park, 2014; Vance, Siponen, and Pahnila, 2012; Workman, 2009). Contradictory findings from previous studies could be due to cultural differences. Thus, in recommendations for future information security research, the need for cultural or context-specific research was outlined (e.g., (Crossler, 2013 #104@@author-year)).

ISP compliance is a subcategory of ISB that refers to how individuals react to security threats. Stanton et al. (2005) classified different types of end-user behavior based on the required knowledge and intentions. The intentional destruction of information with malicious intent and low expertise can lead to harmful use, such as spamming, which may cause trouble but has little impact on the company's activities. Malicious intentions can also result in unintentional harm to the organization. Hazardous tinkering, such as sharing network connections with outsiders, and naive mistakes, such as using weak passwords, are classified as high or poorly skilled neutral intentions that could be harmful to the organization. These two categories, as well as having strong expertise and low hygiene, are guided by positive intentions and result in knowing assurance, such as detecting security threats or complying with ISP. There has been extensive research into the importance, motivations, and causes of staff's ISP violations.

2.5 Information Security Policy violation.

ISP violation are one of the primary focuses of information security research. Because information security is a major concern for today's organizations, many companies spend a

significant amount of money developing a suitable and effective mechanism that they believe will protect their information security. In this regard, implementing ISP, which contains rules, regulations, guidelines, intentions, and principles, is one of the most well-known security mechanisms (Sommestad et al., 2015). The ISP clearly states what actions should be taken in response to various types of violations and what constitutes acceptable use of information security resources (Li et al., 2021).

ISP violations are defined as "unauthorized access to data and systems, unauthorized transfers or copying of confidential information, or the sale of confidential data to a third party." ISP violations can also be defined as the misuse of IS assets, such as hardware, software, data, and other computer services (Hu et al., 2011). Misuse of assets can damage hardware, cause data misappropriation, or involve unlicensed device use (Eskelinen, 2019). Kraemer and Carayon (2007) also define violations generally as a result of human error. They all agree that ISP violations are "threats to confidentiality, integrity, and access to information."

Regardless of the security policies in place, protecting information systems has become a moving target for most organizations worldwide (Sommestad and Hallberg, 2013). Research on ISP violation is a related research area of information security behavior within the organizational context. Studies in this field assume that measuring and studying ISP violations in organizations is critical. Thus, several studies have been conducted to address the issue of ISPs violation. For example, Hu et al. (2015) consider security violations from a lab-based neuroscience perspective and use event-related brain potentials (Ralston et al.), to study them. Aurigemma and Mattson (2017a) investigated the impact of sanction on effects in a company with a strong information security program. According to the findings, an employee's perception of sanction severity has a significant impact on their intent to comply with the ISP. On the other hand, their perceived certainty of sanction imposition does not have an impact, which supports previous research.

Barlow et al. (2013) examine whether IT security communications, rather than deterrence penalties, will decrease ISP violation intentions. Results show that security communication and training are almost as important as communication that focuses on deterrence penalties in persuading workers not to violate ISPs. Equally compelling are both framing types. Cheng et al. (2013) developed a research model based on social bond and deterrence theories rooted in a

social control perspective to investigate how an internal agent has weaker social bonds. Empirical results highlight the considerable impact of formal and informal controls on employees' intentions to violate ISPs.

Tarafdar et al. (2014) explore the "dark side" of IT usage and suggest that variables such as IT-related tension, job overload, interruptions, addiction, and convictions are motivators to breach (security-related). Sanctions and moral considerations temper these. Internal agents use neutralization techniques to reduce the perceived harm of policy violations, according

Internal agents use neutralization techniques to reduce the perceived harm of policy violations, according to (Vance and Siponen, 2012). Ugrin and Pearson (2010) published observational research on cyber-loafing, accessing, and exposing others to pornographic and sexual content as a means of policy non-compliance.

Warkentin et al. (2012) state that whether the sanctions are positive or negative, they may influence employees across cultures. Interestingly, empirical research in Japanese culture by Takemura (2014) suggests that the threat of sanctions does not always deter violations of ISPs . Researchers Njenga and Lowry (2018) say that using grounded theory in this study shows how people behave in a certain institution and builds a strong theory of intention. According to the model, when there is an imbalance in counterfactual reasoning, it is highly probable that there will be violations of information security policy.

The study by Yazdanmehr et al. (2024) investigates the impact of ethical climates on employee breaches of the ISP within the context of information security. The study categorized instances of ISP misconduct towards shared and interconnected IT assets and examined the impact of different ethical environments on these transgressions. The study discovered that ethical climates based on rules and friendship discourage violations by ISPs, whereas a profit-oriented climate does not have the same effect. The study conducted by Ali and Dominic (2024) reveals the widespread occurrence of technostress in oil and gas organizations. Additionally, the study proposes alternative approaches to mitigate the negative impacts of information security requirements that cause stress. King and Paul (2024) suggest expanding the neutralization model by incorporating the influence of individuals' business orientation and ethical orientation on their inclination to neutralize and make concessions with regards to information security policy.

Yazdanmehr and Wang (2023) employ four scenarios in the survey's findings, which indicate that peer monitoring reduces individuals' inclination to violate ISPs. Moreover, both the concepts of shared accountability and reliance play a role in peer surveillance. Trust ultimately enhances the impact of peer monitoring on employees' inclination to breach ISPs.

The study conducted by (Al-Mukahal and Alshare, 2015) is to analyses the factors that influence the frequency of information security policy violations in organizations in Qatar. Additionally, the study aims to assess how Hofstede's cultural dimensions moderate the relationships between these factors and the number of information security policy violations.

Vance and Siponen (2012) used rational choice and deterrence theory to set up a model to better explain the impact of the expected benefit on the violation of ISPs. This testing found that while informal sanctions had a significant effect on the intention to violate ISP, formal sanctions had no significant impact. Moral beliefs, on the other hand, had a negative effect on the intention to violate ISP. Finally, the study demonstrated that informal sanctions, perceived benefits, and moral beliefs affect employees' non-compliance with ISP.

Li et al. (2021) discovered that situational moral beliefs were the primary factor influencing ISP violations in three different situations within an organizational context. However, the impact of moral beliefs on moderation was only statistically significant in situations that specifically involved sharing passwords and selling confidential data. The effects of sanction certainty and sanction severity varied across different situations.

The study conducted by Kim and Oh (2018) revealed that the information security culture had a significant statistical influence on devaluing the organization. However, its impact on reconstructing the conduct and distorting the consequences was not as pronounced. The behavior of peers in complying with security measures had a substantial influence on the reconstruction of conduct, distortion of outcomes, and devaluation of the organization. These factors also had a relevant impact on the intention of organizational members to violate security policies.

Sarkar et al. (2020) study finding reveals the significant impact of professional subculture on violations of ISP within organizations. The findings offer valuable insights for researchers and managers, which can be utilized to enhance overall compliance with ISP. Vance et al. (2020) research demonstrates that informal sanctions have a noteworthy impact on individuals who

adhere to a collectivist cultural value. Conversely, our multinational sample showed that moral belief, neutralization techniques, and shame had significant effects, indicating that these predictors are not influenced by culture. The results also indicate that the impact of formal sanctions was negligible in all cultures included in their data.

Many of these studies focus on fear-based mechanisms, such as the cost of sanctions, while ignoring the perceived benefits of non-compliance and moral beliefs. Even in studies that include perceived benefits, the results cannot be applied to a broad ISP compliance level. They only cover one type of security policy: the internet use policy. (Vance and Siponen, 2012) argue that various types of security policy violations must be included to make the output generalizable across various information security policy violations. They also recommend future studies on perceived benefits and moral beliefs in various cultural settings.

The factors for violations of security policies research result shown to vary from one study to another. Most importantly, none of the mentioned above information security studies look into the influence of organizational culture on RCT constructs like shame, perceived benefits, and moral beliefs. As a result, our research can address these issues.

2.6 Information Security Compliance

2.6.1 Related works on information security compliance

Information systems scholars have focused on employees' compliance with information security policies for decades and have produced valuable research works that contribute theoretical and practical knowledge to the information security literature (Ifinedo, 2016). This review examines these works, identifies the contributions made so far, and addresses the remaining research gaps.

Research on ISP compliance has identified attitudes towards compliance, subjective personal norms, and perceptions of sanction compliance behavior influencers (Ifinedo, 2018). Like other information security behavioral studies, many theories have been applied to study ISP compliance. Some of these theories include protection motivation theory, theory of planned behavior, rational choice theory, general deterrence theory, behavioral decision theory, social

learning theory , social bond theory, general strains theory, and grounded theory (Sommestad et al.) (Bruno et al., 2017).

Research Title and Authors	**Significant Contribution**	**Research ability Gaps**
Puhakainen and Siponen (2010), Improving employees' compliance through information systems security training.	Proposed theory-based training rooted in two models to enhance ISP compliance. Validated through action research, demonstrating efficacy and practicality.	Lacks detailed exploration of implementation challenges in diverse organizational contexts.
Bulgurcu et al. (2010), Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness.	Explored how rationality-based beliefs and information security awareness influence compliance with policies found they significantly affect employees' compliance behavior.	Investigate the impact of organizational factors on an employee's attitude toward compliance. Incorporate both individual factors and institutional factors in shaping an employee's intention to comply with the ISP.
Johnston et al. (2015), An enhanced fear appeal rhetorical framework.	Challenges in information security. Introduces a new framework incorporating sanctioning rhetoric, enhancing personal relevance and compliance intentions.	Limited exploration of potential drawbacks or contextual effects of fear appeals in security campaigns.
Liang et al. (2013), Ensuring employees' IT compliance: carrot or stick.	Utilizes control theory and regulatory focus theory to analyze regulatory focus, reward, punishment, and compliance behavior relationships.	Limited generalizability due to focus on ERP compliance in specific organizational context. Further research needed to

		validate findings across diverse IT mandates and industries.
Johnston and Warkentin (2010), Fear appeals and information security behaviours: An empirical study.	Investigates the impact of fear appeals on end user compliance with computer security actions. Develops and tests a conceptual model integrating technology adoption and fear appeal theories.	Further research needed to empirically understand how perceptions of self-efficacy, response efficacy, threat severity, and social influence affect compliance. Does not fully explore individual differences in organizations in response to fear appeals.
Boss et al. (2015), what do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviours.	Addresses the need for motivating secure behaviours amidst widespread information security violations. Identifies opportunities to enhance PMT application in security research, particularly in utilizing fear appeals and modelling fear.	Existing studies underutilize PMT constructs, neglect fear-appeal manipulations, and lack modelling or measurement of fear. Limited exploration of actual security behaviours.
Amankwa et al. (2018), Establishing Information Security Policy Compliance Culture in Organizations.	Focus on establishing information security policy compliance culture in organizations.	Limited exploration of the impact of organizational culture on compliance.
Abdul Talib and Dhillon (2015), Employee ISP Compliance Intentions : An Empirical Test of Empowerment Employee.	Empirical testing of employee ISP compliance intentions.	Limited examination of the influence of organizational culture specifically communication culture on compliance intentions.

Yazdanmehr and Wang (2016), Employees' Information Security Policy Compliance : A Norm Activation Perspective.	Examination of employees' information security policy compliance from a norm activation perspective.	Insufficient exploration of the impact of organizational culture like employees norms on compliance behaviour.
Aurigemma and Mattson (2017b), Privilege or Procedure: Evaluating The Effect of Employee Status on Intent to Comply with Socially Interactive Information Security Threats and Controls.	Examination of employees' information security policy compliance from a norm activation perspective.	Limited analysis of the role of organizational hierarchy and culture in influencing compliance intentions.
Aurigemma and Mattson (2017a) Deterrence and Punishment Experience Impacts on ISP Compliance Attitudes.	Investigation into the impacts of deterrence and punishment experiences on ISP compliance attitudes.	Limited examination of the role of organizational justice perceptions on compliance attitudes.
Doherty and Tajuddin (2018) , Towards a User-Centric Theory of Value-Driven Information Security Compliance.	Development of a user-centric theory of value-driven information security compliance.	Insufficient consideration of the impact of cultural factors influencing value perceptions of information security compliance.
Garza and Guo (2015), Securing BYOD : A Study of Framing and Neutralization Effects on Mobile Device Security Policy Compliance.	Study on the effects of framing and neutralization on mobile device security policy compliance.	Limited exploration of the impact of culture on mobile use compliance behaviour.

Humaidi and Balakrishnan (2015) , The Moderating Effect of Working Experience on Health Information System Security Policies Compliance Behaviour.	Investigation of the moderating effect of working experience on compliance behaviour towards health information system security policies.	Limited exploration of the influence of organizational support or culture on compliance behaviour.
Alalwan (2018) , Fear of Cybercrime and the Compliance with Information Security Policies : A Theoretical Study.	Theoretical study on the relationship between fear of cybercrime and compliance with information security policies.	Lack of empirical validation of the proposed theoretical framework in different organizational contexts.
Hina and Dominic (2016), Information Security Policies: Investigation of Compliance in Universities.	Investigation of compliance with information security policies in universities.	Examination of the role of institutional culture in shaping compliance behaviour among university staff and students.
Huang et al. (2016), Willingness and Ability to Perform Information Security Compliance Behaviour: Psychological Ownership and Self-Efficacy Perspective.	Exploration of willingness and ability to perform information security compliance behaviour from a psychological ownership and self-efficacy perspective.	Limited analysis of the impact of organizational training programs on self-efficacy and compliance behaviour.
Cyprian Maphanga and Jokonya (2017) , The Risk of Users' Negative Behaviours on Information Security Compliance Policy in Organizations.	Examination of the risk of users' negative behaviours on information security compliance policy in organizations.	Limited exploration of the role of leadership interventions in addressing negative behaviours and fostering a culture of compliance.

Merhi and Ahluwalia (2015) "Top Management Can Lower Resistance toward Information Security Compliance".	Exploration of the role of top management in reducing resistance toward information security compliance.	Limited consideration of the impact of organizational communication strategies on resistance and compliance behaviour.
Moody et al. (2018) , Toward a Unified Model of Information Security Policy Compliance.	Development of a unified model for information security policy compliance.	Examination of the role of organizational culture in influencing the applicability and effectiveness of the unified model across different organizational contexts.
Talib (2015) Intrinsic Motivation and Information Systems Security Policy Compliance in Organizations.	Investigation into the role of intrinsic motivation in information systems security policy compliance	Lack of analysis on the influence of extrinsic motivators on compliance behaviour in organizational cultural context.
Tsohou and Holtkamp (2018), Are Users Competent to Comply with Information Security Policies? An Analysis of Professional Competence Models.	Analysis of users' competence in complying with information security policies using professional competence models.	Limited examination of the impact of organizational culture, training and support on user competence.
Chen et al. (2018) , Information & Management Sanction Severity and Employees' Information Security Policy Compliance : Investigating	Investigation into the mediating, moderating, and control variables influencing the relationship between sanction severity and employees' information security policy compliance.	Examination of the role of organizational justice perceptions in mediating the relationship between sanction severity and compliance behaviour.

Mediating, Moderating, and Control Variables.		
Choi and Song (2018) , Social Control Through Deterrence on The Compliance with Information Security Policy.	Study on the role of social control through deterrence in compliance with information security policy.	Exploration of the relationship between organizational trust and the effectiveness of deterrence mechanisms in promoting compliance behaviour.
D'Arcy and Lowry (2019), Cognitive-Affective Drivers of Employees' Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study.	Longitudinal study on the cognitive-affective drivers of employees' daily compliance with information security policies.	Investigation into the influence of organizational culture factors (e.g., leadership styles, organizational support) on cognitive-affective drivers of compliance behaviour.
Sharma and Warkentin (2019) , Do I really belong? Impact of employment status on information security policy compliance.	Investigates the impact of employment status on information security policy compliance, shedding light on how different employment categories influence compliance behaviour.	Further investigation into the role of organizational culture and leadership in shaping the relationship between employment status and information security policy compliance could enhance understanding in this area.
Yazdanmehr et al. (2020), Peers matter: The moderating role of social influence on information security policy compliance.	Introduces a social contingency model that examines the moderating effects of social influence, specifically a rules-oriented ethical climate at the organizational level and susceptibility to interpersonal	Limited exploration of the specific mechanisms through which social influence factors interact with command-and-control and self-regulatory approaches to affect ISP compliance.

	influence at the individual level, on ISP compliance.	
Liu et al. (2020), Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment.	Investigates the influence of supervisor-subordinate guanxi (SSG) and organizational commitment on employees' compliance with organizational information security policy (ISP), drawing upon technology threat avoidance theory (TTAT) and social exchange theory (SET).	Further research could explore the applicability of the study's findings in different organizational contexts and cultural settings to ascertain the generalizability of the relationships between SSG, organizational commitment, and ISP compliance.
M. Siponen et al. (2014) , Employees' adherence to information security policies: An exploratory field study.	Developed a new multi-theory-based model that explains employees' compliance to information security policies.	Further research could examine the generalizability of the developed model in various organizational settings across different cultural contexts to validate its effectiveness in explaining employees' compliance to ISP.
Bulgurcu et al. (2010), Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness.	Explored how rationality-based beliefs and information security awareness influence compliance with policies.	Future research might investigate the impact of organizational factors on an employee's attitude toward compliance. Incorporate both individual and institutional factors to explain compliance intention and importance of those factors in shaping an employee's intention to comply with the ISP.

Cram et al. (2019) Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance.	Conducts meta-analysis to identify key factors driving compliance with security policies. Offers insights for theory refinement and practical guidance for compliance management.	Limited exploration of contextual factors and interactions between antecedents. Further research needed for broader validation across different organizational settings.
C. Vroom and R. von Solms, (2004), Towards information security behavioural compliance.	Organisational culture is more effective in changing compliance than traditional policing approaches.	Investigation into the influence of organizational culture factors
Thomson and R. Von Solms (2005), Information security obedience.	Conceptual Information security culture should be embedded into the organisational culture	Limited exploration of developing and testing an empirical model information security culture and organizational culture. By giving focus on the effects of organizational cultures on ISP compliance
Karlsson et al. (2022), The effect of perceived organizational culture on employees' information security compliance.	Organizational cultures with an internal focus are positively related to employees' ISP compliance. Differences in organizational culture with regards to control and flexibility seem to have less effect. The analysis shows that a bureaucratic form of organizational culture is most	Lack of investigating Mediating and Moderating effects of organizational cultures ISP compliance.

	fruitful for fostering employees' ISP compliance.	
Solomon and Brown (2021), The influence of organisational culture and information security culture on employee compliance behaviour.	Organisational culture and information security culture have significant, yet similar influences on employee compliance. In addition, organisational culture has a strong causal influence on information security culture.	Future research might investigate the impact of organizational culture on an employee's ISP compliance. Instated of information security subculture
Tang et al. (2016), The impacts of organizational culture on information security culture: a case study.	Organisational culture influences an information security compliant culture. Culture theory used Hofstede et al. (1990)	Limited exploration of the Mediating and Moderating effects of organizational cultures on ISP compliance using other culture theories.
Butler and Brown (2023), COVID-19 pandemic-induced organisational cultural shifts and employee information security compliance behaviour: a South African case study.	The COVID-19 pandemic created a sudden shift to work-from home for employees, and relatedly an increase in cybercrime. The organisational response to this gave rise to shifts in both organisational and information security culture towards greater control and greater flexibility most significantly with information security culture flexibility. The net effect was an increase in employee information security compliance.	Future research might investigate the impact of organizational culture on an employee's ISP compliance. Instated of the combined influence of organisational culture and information security culture on employee ISP compliance. Limited exploration of the Mediating and Moderating effects of organizational cultures on ISP compliance

Table 2. 1 Table List of related works

2.7 Culture

Culture is a broad-ranging term with a theoretical basis that covers many subjects, including psychology, management, anthropology, and other sciences. Culture has been used to identify cultures and national or geographical communities (Hofstede, 1984). However, early writers took up the phrase in organizational studies because it can be applied to other human categories, such as organizations. As defined by (Plog et al., 1976), culture "is a system of shared beliefs, values, customs, behaviors, and artefacts that are transmitted from generation to generation through learning, which members of society use to cope with each other and with their world." (Hofstede, 1984) defines culture as "the collective mental program, which distinguishes between members of one human group and another... the interactive group of common features influencing human groups' environmental response."

Culture has been presented as a factor affecting individuals' success, the implementation of information technology, the incorporation of information systems, information security management, knowledge sharing, and change management. Behavior is closely related to an individual's values and is related to their particular culture (Vance et al., 2020). Jan et al. (2022) argued that culture profoundly affected how information technology technologies were interpreted, used, and adapted.

At different levels, culture may also be defined: at domestic, organizational, and group levels. (Hofstede, 2011) states that it is necessary to distinguish national cultures from organizational cultures. Studies have shown that the different roles played by cultural manifestations are different from national culture to organizational culture. The other difference is that national culture represents values that dominate the entire nation, and organizational culture represents values that dominate a particular organization. (Hofstede, 2011) argues that there can be a correlation between employee behavior and organizational culture. The assumption that organizational culture is not developed independently of the nation's culture (Hofstede, 2011) highlights how one level of culture affects another. In the literature and among practitioners, the two possibilities are evident.

For example, (Hofstede, 2011) argues that culture defines the values of an organization and its members, and that culture forms part of organizational culture. In other words, the national culture in which the organization operates strongly influences organizational values. (Nelson and Gopalan, 2003), on the contrary, argue that the influence of national culture on the values of its members may be overridden through organizational culture. The two views seem to be mid-positioned by (D. Straub et al., 2002), arguing that cultures differ from one another at different times.

These views, combined with the underlying dynamics of organizations, indicate that scholars follow a diverse method of cultural exchange in organizational studies. Indeed, knowing cultural standards at all levels, in tandem with other information technology systems management antecedents, will help to improve the information security standards of organizations. In this report, the emphasis will be on the organizational level and its effect on compliance with information security policies. The assertion of organizational cultural traits impacting information security policy compliance will be further addressed in the following sections.

2.7.1 Organizational Culture

Given the existence of various studies in the area of organizational culture, there is no consensus about one definition of organizational culture as there are divergent viewpoints about this concept. Organizational culture is a collection of the most important values, beliefs, standards, and behavioral norms shared by the majority of members in an organization. (Alharbi and Abedelrahim, 2018; Meng et al., 2016). A significant amount of research is dedicated to studying the values of an organization, which serve as a tangible manifestation of its culture (Alharbi and Abedelrahim, 2018).

Organizational culture is characterized by a collection of values that are “widely shared and strongly held” (Chatman and Jehn, 1994). In another definition, organizational culture can be defined as the distinctive character or identity of an organization, which is formed by a set of commonly held fundamental assumptions, values, beliefs, and practices (de Boer and Goedegebuure, 2014). These elements develop within an organization to fulfill its purpose and address its challenges. Schein (2010) suggested three separate levels of organizational culture: artefacts, assumptions, and values because it has a significant impact on various aspects of

organizational behavior. Another definition was highlighted: “organizational culture is expressed in the principles, the prevailing leadership types, vocabulary and symbols, processes and routines, and the meanings of performance that make an organization special" (Quinn, 2011).

Organizational culture is a broad term that includes different perspectives. Pfister (2009) lists four general characteristics that can benefit when attempting to express what organizational culture is. Firstly, it is about common understandings among group participants, e.g., how tasks should be carried out. Secondly, organizational culture can be reflected in how the company members behave, especially how they collaborate with each other in the organization. Thirdly, organizational culture includes intangible concepts, understandings, and values in the organization. The last trait is the organization's background and culture, which applies to traditions passed down from generation to generation and changes over time (Pfister, 2009).

A definition of organizational culture that captures the key elements from various models is described below: Organizational culture is "a pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and thus, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems" (Schein, 2010).

In general, organizational culture is viewed as a collection of assumptions, ideals, attitudes, and traditions that all members of the organization can share. In this study, we define organizational culture in terms of the values that "represent a manifestation of culture that signifies espoused beliefs identifying what is important to a particular cultural group" (Leidner and Kayworth, 2006), which is similar to the definition by Tsui et al. (2006) that organizational culture is "a set of core values consensually shared by organizational members." To operationalize these shared beliefs and values, which are assumed to be the manifestation of the underlying organizational culture, we adopted the CVF based on prior studies about organizational culture (K. S. Cameron, 1985; Denison et al., 2004; Ernest Chang, 2007; Hu et al., 2012; Quinn and Spreitzer, 1991).

2.7.2 Organizational Culture and Employee Behaviour

In his explanation of culture, Schein (2004) demonstrated that it is both a dynamic phenomenon, which we are constantly engaged in through our interactions, and a set of structures, routines, rules, and regulations that guide and limit our behavior. Thomson et al. (2006) add to this point

by stating that the relationship between organizational culture and employee behavior must be considered when implementing information security practices. It influences employee behavior, limits their work, and dictates what they and the organization should do. According to Lim et al. (2009) corporate culture serves as a mechanism to guide and shape employee behavior.

Triandis and Suh (2002) demonstrate the importance of culture in their work, "Cultural Influences on Personality," despite the fact that behavior is determined by the interaction between personality and situation, not just personality and culture. Many researchers, including Dhillon et al. (2000), Schlarman (2001), and Thomson et al. (2006), have emphasized the significance of understanding organizational culture, such as beliefs, values, and assumptions, in policy and action for the user. Hofstede et al. (1990) suggest that organizational culture is taught at work through socialization, and much of the socialization process is incorporated into the organization's normal work routines for most newcomers.

Therefore, newcomers do not need special training or indoctrination sessions to learn important cultural assumptions; these become obvious through daily conduct. Schlienger and Teufel (2002) also suggest that security culture promotes all activities to make information security a natural aspect of every employee's daily activities. This study shares the view that the culture inside the organization has the most influence on employees' beliefs and attitudes. Thomson et al. (2006)

To create an effective information security environment, it is essential to understand employee behavior and the relationship between information technology, information systems, and organizational culture, which is seen as a driving factor supplying the criminal with the motivation, means, and ability to misuse the mechanism and trigger a breach of information security (Hooper and Blunt, 2020) (Willison and Backhouse, 2006).

The focus of this study is employee security, which is defined as behavior that can have security implications when employees use organizational information systems, including hardware, software, and other systems. Examples of employee security behavior are the way employees handle their passwords and handle corporate data. Besides, the purpose of this study is to differentiate between positive and negative behavior, specifically compliant behavior (i.e., adherence to organizational information security policies, procedures, and norms). Similarly, organizational culture has been conceptualized in terms of values that differentiate one

organization from another. Organizational culture research has been exposed to a wide range of values (Leidner and Kayworth, 2006). This study focuses on organizational cultural traits such as innovativeness, cooperativeness, consistency, and effectiveness.

Organizational culture plays a significant role in shaping employee behavior, especially in the context of compliance with information security policies. Research indicates that organizational culture has similar influences on employee compliance behavior. Furthermore, the creation of a culture specifically focused on information security within an organization can help promote compliance. It's important to note that for information security compliance to be effective, the dominant organizational culture must be taken into consideration. This means that the overarching values, beliefs, and practices that characterize an organization will significantly influence how information security policies are perceived and followed by employees (Solomon and Brown, 2021).

2.7.3 Measuring Organizational Culture

Regular evaluations of the organizational culture and values that dominate the business environment are essential to understanding the factors that contribute to having a negative impact on the way the company operates. Organizational cultural evaluations must be done not only annually but as regularly as possible. Several types of evaluations allow leaders to look at the organizational culture from different perspectives.

As discussed above, numerous definitions, models, and points of view have been proposed for research into how to measure organizational culture. Organizational culture has many elements that contribute to the whole due to the complexity inherent in organizational social systems.

As culture is considered a key factor in organizations, measuring organizational culture becomes important. In response, a range of tools have been developed and applied in industrial, educational, and medical environments in the last two decades to measure organizational culture. While many assessments focus on the surface-level "climate" of an organization, the competing values framework delves deeper. It's a powerful tool that analyzes the underlying values and beliefs shaping an organization's culture.

Nowadays, the CVF is the dominant model in quantitative research on organizational culture, as Kwan and Walker (2004) have pointed out. Many empirical studies on the reliability and validity of the CVF have been published. In this study, an organizational culture assessment was made based on the competing values framework. We used the CVF-based organizational culture assessment instrument (OCAI) to evaluate organizational culture. This scale was used in several previous studies examining different research settings and contexts. For instance, Ernest Chang (2007) measured an organization's culture in terms of four cultural features (cooperative, innovative, consistency, and effective) to examine the relationship between organization culture and ISM and link these features to four information technology security structures (confidentiality, integrity, availability, and responsibility) in a fully connected model.

The CVF model provides a metric that can be used for multicultural, organizational, and cultural analyses. Howard (1998) concluded that the perspective of competing values offers a valid metric to understand, compare, and assess organizational cultures with other variables. Standardized quantitative measures like the ones used in this study are suitable for assessing cultures. Due to its applicability and capacity to systematically measure organizational culture, we have chosen the competing cultural values. Finally, attributing organizational-level values to an individual (without measuring these values at the individual level) may be ecologically invalid (Robinson, 2009). Rather than assuming that individuals within a particular organization all adhere to the same cultural values, it is more accurate to gather cultural values directly from individuals.

This approach allows for a more precise understanding of the cultural influences on behavior. By gathering individual cultural values, researchers can avoid the potential pitfalls of generalizing cultural attributes based solely on national or regional demographics. Instead, they can analyses how these values manifest at the individual level and how they influence behavior. Following this logic, we conceptualize the influence of culture at the individual level, consistent with (Ernest Chang and Lin, 2007; Hu et al., 2012; Srite and Karahanna, 2006; Vance et al., 2020).

2.8 Organizational Culture and Information Security compliance

Over the past few years, information security compliance and organizational culture have been extensively studied. Each field of research has examined, recorded, and published a wealth of information to support the constructs, models, and theories developed and tested. In the literature of information security, studies have been published that examine the role of organization culture on information security compliance although there are only a few papers in the existing literature that acknowledge the link between information security compliance and organizational culture (Butler and Brown, 2023; D'Arcy and Greene, 2014; Ernest Chang and Lin, 2007; Hu et al., 2012; Interligi, 2010; Lim et al., 2009; Solomon and Brown, 2021; Tang et al., 2016; Thomson and Von Solms, 2005; Van Niekerk and Von Solms, 2010; Von Solms and Von Solms, 2004; Vroom and von Solms, 2004) they also stated that since the concept of compliance behavior is complex (Ifinedo, 2014) additional research is required to examine the interaction between compliance and organizational cultures (Vance et al., 2020). These indicate the demand for more studies in this area. Hu et al. (2012) concluded that the effect of organizational culture, "one of the primary structures of corporate and human behavior literature," on information security has not been fully studied. The subsequent paragraphs present the findings of the aforementioned studies.

Von Solms (2006) presented the key finding of the study: in order to achieve compliance, it is crucial for company policies to be deeply ingrained in the company culture. Moreover, Vroom and von Solms (2004) proposed that organizational culture is more effective in influencing compliance than conventional policing methods. Transitioning to the next point, the research conducted by Thomson and Von Solms (2005) suggests that it is crucial for an organization to integrate corporate governance and information security policies into its organization’s culture.

In addition, they suggest that this process should commence with senior management. Lim et al. (2009) proposed a conceptual framework, emphasizing that the incorporation of an information security culture should be embedded within the organizational culture. Moving forward, the study conducted by Hu et al. (2012) was based on empirical evidence and concluded that the involvement of top management in information security has a noteworthy impact on organizational culture, which in turn indirectly affects compliance.

Further, in Ernest Chang (2007) study, it was found that the control-oriented constructs, consistency and effectiveness, have a significant influence on all four ISM values. However, the flexibility-oriented constructs, innovativeness and cooperativeness, do not have the same impact. In his doctoral dissertation study, Whipple (2015) investigated the impact of the organization culture values of cooperativeness, innovativeness, consistency, and effectiveness on the information security management concepts of confidentiality, availability, integrity, and accountability. Moreover, this research is based on Ernest Chang (2007) study of the Taiwanese population, while this study is centered on the American population, and this analysis found similar findings. This means that flexible organizations do not put the same emphasis on the ISM values as controlling organizations.

Additionally, Van Niekerk and Von Solms (2010) stated that an understanding of information security forms the foundation for the creation, principles, and beliefs of an information security culture. Adding to this, the study conducted by D'Arcy and Greene (2014) yielded a significant finding, suggesting that an organization's compliance to information security protocols is heavily influenced by its culture.

Finally, Tang (2016) conducted an empirical study that found evidence suggesting that organizational culture has an impact on the development of a culture that complies with information security measures.

In general, the literature review indicates a strong association between information security compliance and organizational culture, which is pivotal for establishing robust ISP compliance. Organizations prioritizing a security-centric culture typically encounter fewer security incidents and exhibit enhanced adaptability to emerging digital threats.

However, many information security studies predominantly depend on fear-based mechanisms to ensure security compliance, neglecting essential factors such as perceived benefits and moral beliefs, as evidenced by Tilahun and Tibebe (2017). Other researchers, like Cram et al. (2019) and Johnston et al. (2015), have also noticed that the theories of planned behavior, general deterrence, agency, and PMT have given mixed and inconsistent results when it comes to their ability to predict behavior and the situations in which they are valid. Cram et al. (2019) and Johnston et al. (2015).

Besides, the effectiveness of sanctions on ISP compliance exhibits inconsistent and contradictory results, as also indicated by (Cram et al., 2019; D'arcy and Herath, 2011; Vance et al., 2020). Critical elements like shame and informal sanctions have received inadequate attention or investigation, this claim aligns with previous research (Tilahun and Tibebe, 2017). The analysis also reveals uncertainty regarding whether organizational culture directly influences information security outcomes or if its impact is mediated or moderated by other individual or organizational-level factors. Additionally, there is a notable lack of research on ISP compliance in developing countries or within the context of information and communications technologies for development (ICT4D). Contextual factors like organizational culture are often less considered in ISP compliance studies.

2.9 Theoretical Framework

In the exploration of the intricate dynamics shaping individuals' decisions regarding information security compliance within organizational settings, the theoretical framework section of this study delves into two pivotal perspectives: RCT and CVF. These theoretical lenses provide a comprehensive framework for comprehending the nuanced interplay between individual rationality and organizational culture. By integrating these perspectives, this study seeks to shed light on the multifaceted nature of information security compliance.

The subsequent sections will delve into rational choice theory and the competing values framework, providing a detailed analysis of their principles and applications in understanding decision-making processes within organizations, as well as how they shape organizational culture and values.

2.9.1 Rational Choice Theory

The rational choice theory was initially proposed by Becker (1968), with the underlying premise that individuals make choices that enable them to attain their goals and optimize their overall satisfaction. In another work by, Raymond Paternoster and Simpson (1996) model of corporate crime RCT uses economics to explain how people make decisions when confronted with options. Moreover, the intent to commit undesirable action within an organizational setting is determined by the actor's perceived benefits, the potential severity of sanctions, moral values, perceptions of prestige, and the potential for asset loss to the organization. RCT boasts two fundamental

assumptions. First, illegal actors consciously consider the benefits and punishment of deviant actions before they act. Second, the decision to act may be determined by perceptions of cost calculations against potential benefits (Li et al., 2018).

Research conducted in various fields demonstrates that the theory of rational choice theory is more applicable in explaining white collar crime compared to street level crime (Cao, 2004). Therefore, it would be beneficial to utilize this theory in order to provide a more comprehensive understanding of employees' compliance behavior with the information security policy. Researchers across various disciplines, such as politics, labor markets, formal organizations, and criminology, have recognized the significant impact of RCT and employed this theory to examine numerous social issues within their respective fields.

A growing body of research has been addressed to clarify human information security behavior, and several theories have been applied to mention some D'Arcy et al. (2009) used GDT, and Bhatti et al. (2021) used AT. Herath and Rao (2009) used PMT. Pahnila et al. (2007) combine the PMT and GDT. Kuppusamy et al. (2022) assert that the theories of planned behavior and protection motivation theory are the two major theories dominating information security compliance studies.

However, many empirical studies that are conducted to investigate individuals' information security compliance were mainly focused on fear-based strategy and provide only partial insight (Vance et al., 2012). Furthermore, RCT includes additional constructs such as perceived benefits and moral beliefs that provide a holistic view of the behavioral information security problems (D'arcy & Herath, 2011). RCT provides a framework for understanding decision-making, focusing on cost-benefit analysis. Yet, decisions are not solely based on cost-benefit analysis but also on personal values, emotions, social norms, etc. RCT offers a comprehensive perspective on information security by considering individual perceptions of compliance benefits or costs, informal and formal sanctions, and moral values.

We can cite studies (Bulgurcu et al., 2010; D'Arcy and Lowry, 2019; Han et al., 2017; Khatib and Barki, 2022; Li et al., 2010; Vance and Siponen, 2012) that surpass the usual standards and incorporate additional elements of the RCT, such as perceived benefits and moral beliefs, into their empirical research. When examining their impact on the field of information security, they

primarily introduced the RCT theory to the area of ISP compliance, which is a remarkable contribution.

When applied to investigate the moderating role of organizational culture in information security compliance, RCT leverages its strength in understanding rational decision-making processes. RCT can be used to look at different aspects of compliance behavior, such as incentives (perceived benefits), disincentives (formal and informal sanctions), and the new way that moral beliefs are being used in utilitarian calculations (M. Siponen et al., 2010). These aspects are crucial for understanding how actions significantly influence the impact of organizational culture on compliance.

This approach offers valuable insights into the rational decision-making processes of employees regarding information security and how organizational culture can either facilitate or hinder compliance efforts. Furthermore, researchers have not thoroughly studied all RCT constructs in the African context, and they have rarely investigated the concept of shame in relation to employees' ISP compliance (Tilahun and Tibebe, 2017).

Our research seeks to address these gaps by examining ISP compliance behavior using RCT as a theoretical model. Consequently, our model incorporates moral beliefs, shame, formal sanctions, informal sanctions, and perceived benefits into the decision-making process, as shown in Figure 2.1. As a result, we consider the application of RCTs as one of our theoretical lenses to be both appropriate and justifiable. The other major theory we used in this study is organizational culture. Hence, in the next section, we discuss the competing values framework in detail.

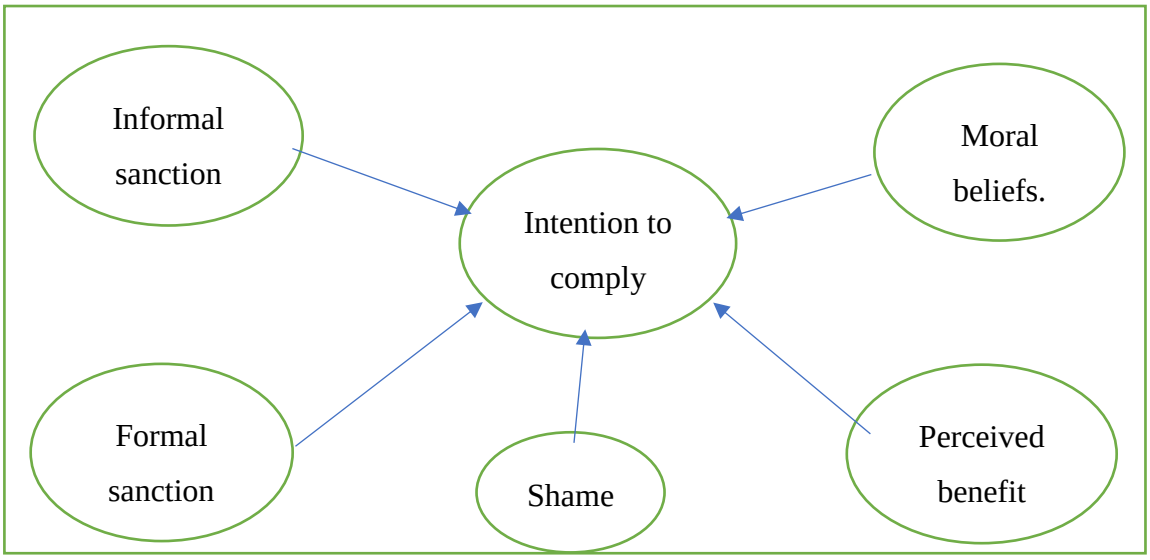


Figure 2. 2: The Rational Choice Theory

2.9.2 Organizational Culture and Competing Values Framework

In recent decades, several scholars have proposed various dimensions of organizational culture that can be used to describe organizational practices. These scholars include House et al., Denison and Mishra, O'Reilly et al., Gordon and DiTamaso, Detert et al., Van Muijen et al, Hofstede, and others. For example, Kennedy (1982) introduced the concept of organizational culture, which is based on feedback and risk measures.

They categorized organizational culture into four dimensions: bet your company culture, work/hard/play complex culture, tough-guy macho, and process culture. Schein (1983) categorized organizational culture into three distinct dimensions: assumptions, values, and artifacts. O'Reilly III et al. (1991) introduced the organizational culture profile, a tool that examines distinct aspects of organizational culture, including attention to detail, a result-driven mindset, regard for people, an emphasis on teamwork, and inclination towards innovation. Hofstede et al. (1990) discovered six dimensions in their research: (1) results-oriented versus process-oriented; (2) employee-oriented versus job-oriented; (3) parochial versus professional; (4) closed systems versus open systems; (5) loose versus tight control; and (6) normative versus pragmatic.

Another model for measuring organizational culture was Denison's (1990), which has four dimensions: involvement, adaptability, consistency, and mission. Detert et al. (2000) proposed an eight-dimensional model for measuring organizational culture, which includes (1) the basis of truth and rationality in the organization; (2) the nature of time and time horizon; (3) motivation; (4) stability versus change/innovation/personal growth; (5) orientation to work, tasks, and co-workers; (6) isolation versus collaboration/cooperation; (7) control, coordination, and responsibility; and (8) orientation and focus internal and/or external.

Gordon and DiTomaso (1992) proposed a model for measuring organizational culture that includes the fairness of rewards, action-oriented integration, accountability, systematic decision-making, innovation, and clarity of strategies. Van Muijen (1999) proposed a model that includes goal orientation, support orientation, rule orientation, and innovation orientation.

Among the various theories and models, K. Cameron (2009) Competing Values Framework (CVF) has been widely used in research on organizational culture. The basic principle of CVF is that organizations should be diagnosed as either one or a mixture of four culture types: clan, adhocracy; market; and hierarchy. K. Cameron (2009) created a methodology called, the organizational culture assessment instrument, in collaboration with the CVF. They contended that even though they produced a more extended version of the OCAI, the more parsimonious version was equally indicative of an organizational culture. The CVF and OCAI have been used in more than 1,000 organizations and have been shown to predict organizational success (K. Cameron, 2009).

This research used the CVF because we believe it is the most appropriate framework for measuring organizational culture. We also believe that measuring organizational culture characteristics should be based on empirical evidence and should integrate and organize most of the proposed dimensions. That is the purpose of using the CVF. The CVF is a framework that was empirically derived and has been found to have both face and empirical validity, helping to integrate many of the dimensions proposed by various authors. The CVF is one of the most influential and extensively used models in organizational culture research. The CVF was initially developed based on research conducted on the significant indicators of effective organizations.

Yang and Ryan (2013) indicated that the control-flexibility dimension reflects the extent to which an organization focuses on stability versus change, whereas the internal-external dimension demonstrates the organization's focus on the internal organization versus the external environment. The framework explained that these two dimensions form four quadrants, each representing a distinct set of organizational effectiveness indicators and forming four types of culture.

Compared with the above models, the CVF and its matched scale OCAI have the following advantages: few dimensions but broad implications. The CVF contains only two dimensions while integrating the essence of the eight widely agreed-upon dimensions listed above (Ralston et al., 2006; Yu and Wu, 2009). The two dimensions of control vs. autonomy and internal vs. external are explicitly included in the CVF. Furthermore, three dimensions (stability vs. change, orientation to work/co-workers, and separation vs. collaboration) are specifically merged in the

theoretical model. In addition, the paradigm also discusses, in theory, the other three corporate culture dimensions.

For our research, we think that the most appropriate frameworks for measuring organizational culture characteristics must be valid and should be able to integrate and organize most of the dimensions being proposed; that is, they should simply, be based on empirical evidence; That is one of the purposes of using the CVF. Competing values framework, shown in the figure below, is a framework that was empirically derived, has been found to have both face and empirical validity, and helps to integrate many of the dimensions proposed by various authors (K. Cameron, 2009). The CVF is one of the most influential and extensively used models in the area of organizational culture research (Yu and Wu, 2009).

Besides, Empirical research in the field of culture has extensively tested and confirmed the validity and reliability of the CVF and OCAI. Notable studies by Howard (1998) and Ralston et al. (2006) have provided empirical evidence supporting these findings. The CVF has been widely utilized for various country samples, as demonstrated by studies conducted by Kwan and Walker (2004). The OCAI questionnaire is highly succinct, consisting of only 24 elements, and is particularly useful for practical operations. To summarize the analysis on the CVF, the authors conclude that both the CVF and its matched scale OCAI are highly suitable for quantitative testing. Therefore, we believe that the use of CVF as one of our theoretical lenses is justified and also appropriate.

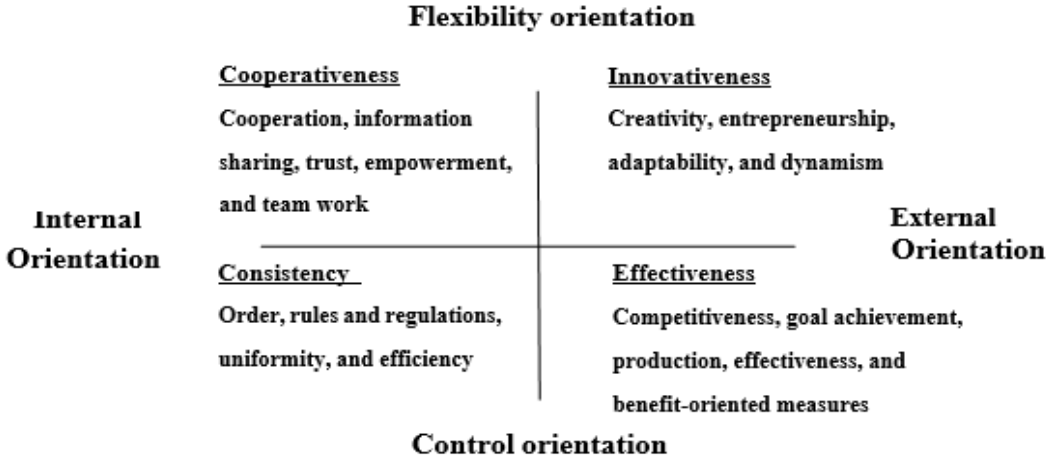


Figure 2. 3 : The model of organizational culture

2.10 Research model and research hypothesis development

We develop a model based on RCT and CVF. From RCT, we include all variables, namely: moral beliefs, perceived benefits, informal sanction, formal sanction, and shame. In addition to this, our model also inculcates four of the organizational culture dimensions, namely: cooperativeness, innovativeness, consistency, and effectiveness. The research model is shown in Figure 2.3 and each of the elements of the model and their corresponding hypotheses are discussed below.

Moral belief

Moral beliefs are the academic background of ethics, and they refer to the interpretation that people have about what is morally right or wrong, which impacts their behavior and intention (Vance et al., 2020). In the context of information security policy compliance, moral beliefs can be seen as an employee's perception of compliance with the organization's information security policy as morally acceptable. The stronger an individual's moral beliefs about the importance of complying with the policy, the more likely they are to comply with it (Ejigu et al., 2023).

Several studies have shown that moral beliefs have a significant impact on compliance intentions with information security policies. For example, Vance and Siponen (2012) found that moral beliefs had the strongest impact on compliance intention with ISP in their RCT-based model. Similarly, Li et al. (2010) Li et al. (2010) showed that moral beliefs had a positive effect on compliance intention with internet policies in their RCT-based model. Myyry et al. (2009) also found that people's values and moral reasoning could help predict the information security policy compliance of individuals.

Moreover, Vance et al. (2020) suggested that the influence of sanctions for rule-breaking behavior is dependent on an individual's moral beliefs. Individuals with strong moral beliefs consider rule-breaking behavior as morally wrong, and sanctions may be irrelevant for them. On the other hand, individuals with weak moral beliefs may not view rule-breaking behavior as morally wrong, and the influence of sanctions on them would be considerable. This suggests that

moral beliefs have an overriding influence on final decisions involving deviant and criminal behaviors.

Therefore, we can infer that if an individual perceives noncompliance with the ISP as morally wrong, they are less likely to violate the information security policies. Vance et al. (2020) found that moral beliefs negatively impact information security policy violation intention. In other words, individuals who view information security policy violations as morally wrong are less likely to violate the ISP. In conclusion, the hypothesis that moral beliefs have a significant positive effect on information security policy compliance intention is supported by several studies. Given this theoretical and empirical support, we hypothesize the following:

H1: Moral belief is positively related to employees' intention towards ISP compliance.

Perceived Benefits

Perceived benefits refer to when people engage in a rational decision-making process. First, they come up with the available number of choices and then analyses the outcome of each of the alternatives to choose the one that is perceived to bring more satisfaction or perceived benefits (Ray Paternoster and Pogarsky, 2009). In addition, studies conducted based on the RCT also show that perceived benefits have been found as a good predictor of compliance (Sommestad et al., 2014; Vance and Siponen, 2012). In other words, ISP compliance is positively related to the response to behavior, taken as personal benefits accruing from complying with ISPs in organizational settings (Tyler and Blader, 2005).

Empirical research that uses RCT suggests criminal thoughts include calculations of the perceived benefits of a crime before it is committed. A deviant or illicit act may be more likely to occur if the benefits outweigh the costs, and the potential of detection and punishment is low (Moody et al., 2018). Perceived benefit shows to significantly determine compliance behavior in empirical information security research (Ifinedo, 2016). Besides, perceived benefit affects ISP compliance behavior in empirical information security literature (Ifinedo, 2016).

In information security studies, time-saving has been recognized as a major motivation not to comply with information security policies. Puhakainen and Siponen (2010) findings showed that ISPs were perceived to slow down work with the addition of procedures. Participants in this

study perceived time-saving as a clear benefit of avoiding ISPs. Moreover, Vance and Siponen (2012) reported the significant positive effect of perceived benefits on employees' ISP noncompliance intention. However, Li et al. (2010) studied how employees' compliance intentions for internet usage are driven by cost-benefit assessment factors. Perceived benefits were negatively associated with the intention to comply with the internet use policy. Hence, empirical information security literature suggests perceived benefit construct requires further investigation (Ifinedo, 2016; Moody et al., 2018).

Despite the mixed findings, the literature suggests that perceived benefits play a critical role in shaping employees' compliance intentions with information security policies. Studies have indicated that employees' perceptions of the benefits of complying with information security policies can significantly influence their intentions to comply with those policies (Yang & Lin, 2009). The mixed findings serve as motivation for the current study on the analysis of perceived benefits in RCT.

In conclusion, perceived benefits play a crucial role in employees' decision-making processes when it comes to complying with information security policies in organizational settings. Based on the literature, it can be hypothesized that perceived benefits have a significant positive effect on employees' information security policy compliance intention, and employees who perceive the benefits of complying with information security policies are more likely to comply with them, feel a sense of personal responsibility, and report any security breaches or incidents. We hypothesize the following:

H2: Perceived benefit of compliance is positively related to employees' intention towards ISP compliance.

Formal Sanctions

Formal sanctions refer to specific penalties imposed by society, such as fines or imprisonment for criminal acts, or by employers, such as demotions or termination of employment, for violating policies. Formal sanctions, as defined as explicit punishments levied on particular acts of misbehavior, are a key element of deterrence policy in the rational choice theory (Vance et al., 2020). RCT suggests that individuals make decisions based on a cost-benefit analysis, where the potential benefits of a behavior are weighed against the potential costs of that behavior

(Ifinedo, 2016). In the context of information security policy compliance, formal sanctions may increase the perceived costs of non-compliance, thus influencing employees to comply with information security policies (Chen et al., 2018).

Several studies have examined the relationship between formal sanctions and information security policy compliance. For example, Zhang and Liu (2015) found that the presence of formal sanctions, such as warnings and penalties, significantly increased employees' compliance with information security policies. Similarly, Ejigu et al. (2023) also found that formal sanctions was a significant predictor of employees' intention to comply with information security policies.

However, the effectiveness of formal sanctions may vary depending on the severity and certainty of punishment. D'Arcy and Hovav (2009) reported that formal sanction severity had a significant effect on users' intentions to commit computer abuses. Aurigemma and Mattson (2017a) found that sanction had a significant impact on employees' intent to follow ISP. Moreover, Vance et al. (2020) formal sanctions doesn't have a meaningful influence on employees' intention to comply with the ISP.

Interestingly, the inconsistent findings regarding the impact of formal sanctions on ISP compliance suggest a need for further investigation in empirical studies (Vance et al., 2020). Therefore, the varied findings serve as a motivation for the current study on the analysis of formal sanctions in RCT.

However, the theoretical underpinnings of RCT and the empirical evidence suggest that formal sanctions are an effective tool in promoting information security policy compliance in organizations. It is also important to note that formal sanctions should be used carefully and in conjunction with other measures, such as training and awareness programs, to promote a culture of security and compliance in organizations (Vance et al., 2020). Following the above discussion, we hypothesize that:

H3: Formal sanction is positively related to employees' intention towards ISP compliance.

Informal Sanctions

The effectiveness of formal sanctions in deterring individuals from deviant behavior has been extensively studied and documented in literature (Vance et al., 2020). However, informal

sanctions are unspoken social consequences for undesirable actions, such as the disapproval of friends or peers, social censure, or embarrassment that govern behavior within an organization (Tadesse et al., 2021; Vance and Siponen, 2012), have received less attention in the context of information security policy compliance intention. The hypothesis suggests that informal sanctions have a significant positive effect on information security policy compliance intention.

Theoretical support for this hypothesis can be found in social control theory, which suggests that individuals are motivated to comply with social norms and rules due to the fear of social sanctions (Ejigu et al., 2023). In the context of information security policy compliance, informal sanctions such as peer pressure, social disapproval, and loss of trust can serve as powerful motivators for individuals to comply with information security policies.

Empirical studies have also provided support for this hypothesis. Niu and Guo (2019) conducted a study that found that informal sanctions such as feedback from colleagues and superiors had a significant positive effect on employees' intention to comply with information security policies. Similarly, Liu, Ma, and Zhang (2020) conducted a study that found that perceived social pressure had a positive effect on employees' intention to comply with information security policies.

Furthermore, Yu and Lu (2016) conducted a study that found that social control mechanisms, including informal sanctions, were more effective in promoting information security compliance. This highlights the importance of informal sanctions in promoting information security policy compliance.

Some researchers have suggested that informal sanctions have little impact on ISPs compliance (Li et al., 2010; Pahnila et al., 2007; Vance et al., 2020). However, studies on information security have shown the influence of informal sanctions in reducing noncompliance (M. Siponen et al., 2007; Trang and Brendel, 2019). Empirical information security literature suggests that the RCT construct of informal sanctions requires further investigation in ISP compliance behavior studies (Ifinedo, 2016; Vance et al., 2020). Hence, the diverse results provide motivation for the present study on the examination of informal sanctions in RCT.

In conclusion, based on the theoretical and empirical support, it can be hypothesized that informal sanctions have a significant positive effect on information security policy compliance intention. Incorporating informal sanctions, such as peer pressure and social disapproval, in

information security policies can promote compliance among employees. Organizations can benefit from recognizing the importance of informal sanctions and utilizing them to enhance information security policy compliance.

H4: Informal sanction is positively related to employees' intention towards ISP compliance.

Shame

Shame is an emotional response characterized by a sense of guilt or embarrassment that arises when others become aware of one's socially unacceptable behavior (Vance et al., 2020). Moreover, the concept of shame has been the subject of theoretical analysis and empirical investigation in the disciplines of criminology and psychology. Within the field of criminology, shame is occasionally considered to be a component of deterrence theory, functioning as a form of self-imposed punishment (D'arcy and Herath, 2011). Nevertheless, some criminology scholars have raised doubts regarding the compatibility of shame with the theoretical principles of deterrence theory, which revolves around the concept of intentionally avoiding pain. Due to the criminology and deterrence background, we have incorporated shame as a component in our model. Study on shame has been a prominent area of study for the last 25 years. Scholars have regarded shame as a concept that applies universally and operates through self-assessment of emotions (Vance et al., 2020).

The available literature suggests that shame may have a significant positive effect on information security policy compliance intention. Studies have shown that shame can be a powerful motivator for behavior change, especially in situations where a person's reputation is at risk (Willison and Warkentin, 2013) (Lickel et al., 2014). The perception of the seriousness of the policy and the consequences of non-compliance may increase due to shame. Vance et al. (2020), suggests that feelings of shame have a detrimental effect on employees' intentions to violate an information security policy. In other words, when employees experience shame, it tends to discourage them from engaging in behaviors that would breach or violate the ISP. M. Siponen et al. (2012) study indicates that there was a notable impact of shame on the intention to engage in software piracy. Building upon prior research on shame, our hypothesis posits that shame has the potential to impact information security behavior in the following manner:

H5: Shame is positively related to employees' intention towards ISP compliance.

Consistency culture

Consistency culture, characterized by stability, control, and efficiency. Organizations exhibiting a consistency culture prioritize adherence to rules, procedures, and standards, fostering a climate of orderliness and predictability (Ernest Chang and Lin, 2007). In such cultures, there is a concerted effort to ensure that behaviors and decisions consistently reflect the organization's espoused ethical principles. This includes order, rules, and regulations: this implies a structured environment where there are clear guidelines, protocols, and procedures in place to govern behavior, processes, and interactions.

It suggests that people are expected to follow these rules meticulously to ensure smooth operations and prevent chaos or confusion (Ernest Chang and Lin, 2007; Hu et al., 2012; Whipple, 2015). Uniformity: in a consistency culture, there is a focus on standardization and sameness. This could apply to various aspects such as behavior, services, or outcomes. The aim is to minimize variations and ensure consistency (Ernest Chang and Lin, 2007; Hu et al., 2012; Whipple, 2015). Efficiency: This highlights the importance of optimizing resources, minimizing waste, and achieving desired outcomes with minimal effort or cost. In a culture of consistency, efficiency is valued as it helps in meeting objectives consistently (Hu et al., 2012).

Conversely, moral belief is predicated on individuals' perceptions of what is morally wrong or right. These beliefs heavily influence behavior, particularly in ethical decision-making contexts (Vance et al., 2020). Compliance intention, on the other hand, refers to an individual's willingness or commitment to adhere to ethical standards, rules, or regulations within a specific context, such as organizational policies (Hu et al., 2012). The hypothesis posits that consistency culture enhances the positive relationship between moral beliefs and compliance intention. This assertion is grounded in several factors:

Firstly, as stated above, consistency culture, with its emphasis on order, rules, and regulations, serves as a structured environment where there are clear guidelines and protocols governing employee behavior (Hu et al., 2012). This structured framework minimizes ambiguity and uncertainty, reducing the likelihood of cognitive dissonance between moral beliefs and actions. Individuals operating within such environments experience less internal conflict when their

moral convictions align with the prescribed rules and regulations, leading to a stronger commitment to compliance.

Secondly, within consistency cultures, the emphasis on uniformity extends beyond mere adherence to rules and regulations to encompass behavioral consistency across individuals and organizational levels. Observing consistent ethical conduct reinforces the importance of moral beliefs and strengthens individuals' resolve to adhere to ethical standards, thereby bolstering compliance intentions. Thirdly, consistency culture fosters trust and stability by promoting uniformity and adherence to established norms. Clear rules and regulations provide a sense of predictability and security, fostering an environment where individuals feel confident in expressing their moral beliefs without fear of arbitrary or capricious decision-making. This trust facilitates collaboration and reinforces the link between moral beliefs and compliance intention through collective commitment to upholding ethical standards (Ejigu et al., 2023; Ernest Chang and Lin, 2007; Hu et al., 2012; Solomon and Brown, 2021; Tsai, 2011; Whipple, 2015).

Furthermore, consistent adherence to organizational values within a unified culture nurtures a disciplined, compliant, and performance-oriented workforce (Tsai, 2011). In the context of information security and compliance behavior, a consistent and uniformly enforced organizational culture is expected to create an environment conducive to compliance, leading to an acceleration in compliance intentions. Thus, employees within a consistent culture are expected to react to moral beliefs more responsively and with a heightened sense of intention to conform to compliance norms.

In conclusion, the hypothesis that consistency culture strengthens the positive effect between moral beliefs and compliance intention draws upon the comprehensive evidence from the related literature. The strength of organizational culture consistency in shaping compliance behavior is firmly rooted in establishing an ecosystem where moral norms and organizational values work in harmony to create a culture of compliance. The presence of a consistent and value-driven culture is expected to yield a substantial amplification effect on employees' compliance intentions, bolstered by their strong commitment to organizational ethical norms and values.

Consequently, the hypotheses centered on the relationship between consistency culture, moral beliefs, and compliance intention remain credible, justified, and well-explained. Therefore, following the above assertion, the following hypothesis is formulated:

H6: Consistency culture strengthens the positive effect between moral beliefs and compliance intention.

Effectiveness

Effectiveness culture refers to the organizational culture that emphasizes efficiency, productivity, and achieving goals in an efficient and effective manner. It's characterized by an emphasis on results and continuous improvement (Ernest Chang and Lin, 2007). On the other hand, perceived benefits refer to how individuals within an organization perceive the advantages or positive outcomes associated with a particular action or behavior. In the context of compliance, it could be the perceived advantages of adhering to certain rules, regulations, or protocols (Bulgurcu et al., 2009). Compliance intention denotes an individual's readiness or willingness to conform to rules, regulations, or norms within an organizational context (Hu et al., 2012).

The hypothesis posits that within an organizational context, characterized by an emphasis on efficiency and productivity (effectiveness culture), the positive relationship between individuals' perception of benefits associated with compliance and their intention to comply is strengthened. This assertion stems from several factors: Firstly, organizational alignment: which means an effectiveness culture, is often associated with clarity in goals, processes, and expectations (Ernest Chang and Lin, 2007). When there is a strong effectiveness culture, employees are more likely to understand the benefits associated with compliance. This alignment between the perceived benefits and the organizational culture can strengthen the intention to comply. Secondly, enhanced communication: this is to mean that in an effectiveness culture, communication channels are usually clearer and more open (Whipple, 2015). This facilitates the dissemination of information regarding the benefits of compliance. Employees are more likely to grasp the advantages and importance of adhering to regulations when they are communicated effectively within a culture that values effectiveness.

Thirdly, resource allocation: effectiveness cultures often prioritize resource allocation towards initiatives that yield tangible results (Di Stefano et al., 2019). Compliance efforts may receive more support and resources within such cultures, leading to a reinforcement of the perceived benefits associated with compliance. Fourthly, since there is more support and resources to enhance compliance efforts, there is a strong norms and expectations regarding employee compliance. Employees may feel greater social pressure to comply due to the prevailing organizational norms. This normative influence can amplify the positive effect of perceived benefits on compliance intention.

In this way, we argue that organizational culture plays a moderating role and that the alignment between perceived benefits and compliance intention is stronger in places where there is a culture of effectiveness. This understanding holds significance for organizational management, emphasizing the need to foster cultures that not only prioritize efficiency but also reinforce positive behaviors like compliance, ultimately contributing to organizational effectiveness and performance, as hypothesized in

H7: Effectiveness culture strengthens the positive effect between perceived benefits and compliance intention.

Consistency culture

Next, in examining the hypothesis that consistency culture strengthens the positive effect between formal sanctions and compliance intention, it's crucial to delve into the intricate dynamics between organizational culture and formal sanction.

Consistency culture embodies a set of values and norms within an organization that prioritize order, adherence to rules and regulations, uniformity in behavior, and efficiency in operations. This culture shapes the environment in which employees operate, influencing their perceptions, attitudes, and actions. Formal sanctions, on the other hand, represent the explicit consequences established by the organization or society for non-compliance with rules and regulations. These sanctions serve as deterrents, aiming to discourage undesirable behavior and reinforce adherence to established norms (Vance et al., 2020); (Chen et al., 2018).

Now, the hypothesis posits that consistency culture amplifies the effectiveness of formal sanctions in promoting compliance intention among individuals. This assertion stems from the notion that a strong consistency culture fosters a sense of accountability, clarity, and predictability regarding expected behaviors and their consequences (Ernest Chang and Lin, 2007). In such an environment, individuals are more likely to perceive formal sanctions as fair and legitimate mechanisms for maintaining order and maintaining organizational values. Consequently, formal sanctions increase, enhancing their deterrent effect on non-compliant behavior.

To justify this hypothesis, we can draw upon theoretical frameworks such as social learning theory and organizational justice theory. Social learning theory suggests that individuals observe and imitate the behaviors of others, especially when those behaviors are rewarded or punished. In the context of organizational culture, employees are likely to emulate the behaviors that are consistent with the prevailing norms and values. Therefore, in a consistency culture where adherence to rules is highly valued and consistently reinforced, employees are more inclined to comply with established norms to avoid formal sanctions.

Moreover, consistency culture, characterized by its emphasis on order, rules, and efficiency, creates a structured environment where expectations regarding behavior and performance are clearly defined and consistently reinforced. This clarity and consistency provide employees with a framework within which to understand and navigate their roles, responsibilities, and the consequences of their actions.

Besides, formal sanctions represent a tangible manifestation of organizational norms and values regarding acceptable and unacceptable behavior. By explicitly outlining the penalties for non-compliance, formal sanctions establish boundaries and set expectations for conduct within the organization. In a culture of consistency, where adherence to rules is highly valued and consistently enforced, formal sanctions carry greater weight and significance as mechanisms for maintaining order and discipline.

Additionally, organizational justice theory emphasizes the importance of perceived fairness in shaping employee attitudes and behaviors. When formal sanctions are perceived as applied consistently and transparently within a culture that values order and uniformity, employees are

more likely to perceive the enforcement process as fair and legitimate. This perception of fairness enhances the psychological contract between employees and the organization, fostering trust, commitment, and compliance with organizational rules and regulations.

Furthermore, the hypothesis suggests that consistency culture acts as a moderator, intensifying the relationship between formal sanctions and compliance intention. As a moderator, consistency culture enhances the strength or direction of this relationship by influencing the conditions under which formal sanctions are applied and perceived. Specifically, in a consistency, the alignment between organizational values, enforcement mechanisms, and individual behaviors creates a synergistic effect that reinforces the deterrent power of formal sanctions.

In summary, consistency culture acts as a moderator that amplifies the impact of formal sanctions on compliance intentions. As a moderator, consistency culture shapes the conditions under which formal sanctions are applied and perceived, intensifying their deterrent effect on non-compliant behavior. By fostering a culture where adherence to rules is ingrained and rewarded, consistency culture enhances the salience and severity of formal sanctions, thereby increasing their effectiveness in promoting compliance. Thus, we propose the following hypothesis:

H8: Consistency culture strengthens the positive effect between formal sanctions and compliance intention.

The hypothesis that consistency culture strengthens the positive effect between informal sanctions and compliance intention within organizational settings necessitates a robust justification, particularly considering the intricate dynamics between organizational culture, social norms, and individual behavior.

Firstly, as mentioned in the previous hypothesis, consistency culture characteristically fosters a normative environment where adherence to rules and regulations is highly valued and consistently reinforced. Within such an environment, informal sanctions gain amplified influence due to the heightened importance placed on conformity. Individuals are more likely to perceive informal sanctions as significant indicators of social acceptance or disapproval within a consistently structured culture. Therefore, when informal sanctions align with the consistent norms of the culture, their impact on ISP compliance intentions is strengthened.

Secondly, consistency culture establishes a robust framework for social control mechanisms. In environments characterized by order, rules, and regulations, informal social pressures are more effectively leveraged to maintain conformity and discourage deviant behavior. Individuals are more likely to internalize the norms and values of a consistently structured culture, making them more susceptible to the influence of informal sanctions. Consequently, the effect of informal sanctions on compliance intention is heightened within the context of a culture of consistency where adherence to norms is rigorously upheld.

Thirdly, consistency culture facilitates efficient social learning processes wherein individuals acquire and internalize behavioral norms through observation and imitation. Within such cultures, informal sanctions serve as powerful mechanisms for transmitting and reinforcing social norms. Through the consistent application of informal sanctions, individuals learn about the consequences of deviating from established norms and adjust their behavior accordingly to avoid social disapproval. Thus, within a culture of consistency, the impact of informal sanctions on compliance intention is magnified as individuals swiftly adapt their behavior to align with prevailing norms to avoid social penalties.

Lastly, consistency culture fosters a sense of cohesiveness and collective identity among its members, creating a shared commitment to upholding organizational or societal norms. In environments characterized by uniformity and efficiency, individuals develop a strong allegiance to the values and principles that underpin the consistency culture. This collective commitment enhances the effectiveness of informal sanctions by strengthening the sense of social responsibility and accountability among individuals. As a result, the positive effect of informal sanctions on compliance intention is heightened within a consistency culture where individuals are motivated to maintain the integrity of their collective identity by adhering to established norms and values.

Finally, the hypothesis posits that within a consistency culture characterized by order, rules, and uniformity, informal sanctions exert a stronger positive influence on compliance intention due to normative influence amplification, enhanced social control mechanisms, alignment of expectations and behaviors, efficiency in social learning processes, and the cohesiveness of

collective identity. These factors collectively contribute to the heightened impact of informal sanctions on compliance intention within the context of a consistency culture.

H9: Consistency culture strengthens the positive effect between informal sanctions and compliance intention.

Innovativeness culture

Let's discuss the constructs involved. Innovativeness culture, characterized by creativity, entrepreneurship, adaptability, and dynamism, focuses on stimulation, growth, and creativity within organizations (Di Stefano et al., 2019; Ernest Chang and Lin, 2007). This culture fosters an environment where employees are encouraged to think outside the box, experiment with new ideas, and adapt to changing circumstances. In such a culture, individuals are likely to be more open-minded, flexible, and receptive to new approaches and perspectives, including those related to compliance with organizational rules and regulations (Di Stefano et al., 2019; Ernest Chang and Lin, 2007).

Perceived benefits, on the other hand, refer to the outcomes or rewards individuals expect to receive from engaging in a particular behavior or decision-making process. When individuals perceive that a course of action will lead to favorable outcomes or satisfy their needs and preferences, they are more likely to engage in that behavior (Sommestad et al., 2014; Vance and Siponen, 2012). The hypothesis asserts that innovativeness culture strengthens the relationship between perceived benefits and compliance intention. Several factors support this assertion:

To begin with, innovativeness culture fosters an environment that encourages risk-taking and experimentation. Within such a culture, individuals are more likely to perceive the potential benefits associated with compliance as opportunities for innovation and growth. The dynamic and entrepreneurial nature of innovativeness culture motivates individuals to explore new approaches and solutions, viewing compliance as a means to drive positive change and advancement. Consequently, when perceived benefits align with the values of innovativeness culture, their positive effect on compliance intention is strengthened as individuals are inspired to embrace compliance as a pathway to innovation and progress.

Additionally, innovativeness culture is characterized by adaptability and flexibility in response to changing circumstances and environments. Individuals within such cultures are inherently predisposed to recognize and capitalize on opportunities for improvement and development. Perceived benefits associated with compliance are viewed through the lens of adaptability, with individuals recognizing the potential for growth and innovation that compliance entails. As a result, within an innovativeness culture, the positive effect of perceived benefits on compliance intention is magnified, as individuals are motivated to seize opportunities for advancement and adapt their behaviors accordingly to align with evolving standards and expectations.

Moreover, innovativeness culture promotes creativity and out-of-the-box thinking, encouraging individuals to explore unconventional approaches and solutions. Perceived benefits associated with compliance are perceived as catalysts for creative problem-solving and innovation within such cultures. Individuals view compliance as an opportunity to showcase their ingenuity and contribute to the collective pursuit of progress and excellence. Therefore, within an innovativeness culture, the positive effect of perceived benefits on compliance intention is heightened, as individuals are inspired to leverage compliance as a platform for expressing their creativity and driving positive change.

Furthermore, innovativeness culture embodies an entrepreneurial spirit characterized by a keen ability to recognize and seize opportunities for growth and development. Perceived benefits associated with compliance are viewed as strategic advantages that enable individuals to capitalize on emerging trends and market dynamics. Within such cultures, compliance is perceived not only as a means of mitigating risk but also as a pathway to innovation and competitive advantage. So, in an innovative culture, the positive effect of perceived benefits on compliance intention is strengthened, as people are driven to use compliance as a tool for business success and taking advantage of opportunities.

Besides, innovativeness culture is inherently dynamic and forward-thinking, with a focus on continuous improvement and adaptation to changing circumstances. Perceived benefits associated with compliance are evaluated within the context of future-oriented goals and objectives. Individuals within innovativeness cultures recognize the strategic importance of compliance in driving long-term success and sustainability. In an innovative culture, the positive

effect of perceived benefits on compliance intention is amplified because people are motivated to see compliance as a strategic imperative that fits with the culture's dynamic and forward-thinking spirit.

To sum up, the hypothesis says that in a culture of innovativeness marked by creativity, entrepreneurship, adaptability, and dynamism, perceived benefits have a stronger positive effect on compliance intention. This is because these traits encourage people to take risks and try new things, be adaptable and flexible in response to change, be creative and think outside the box, be entrepreneurial and look for opportunities, and be dynamic and forward-thinking. These factors collectively contribute to the heightened impact of perceived benefits on compliance intention within the context of an innovativeness culture. Therefore, we can hypothesize that:

H10: Innovativeness culture strengthens the positive effect between Perceived benefits and compliance intention.

Cooperativeness culture:

Ernest Chang (2007) defined cooperativeness culture that focuses primarily on cooperation, information sharing, trust, empowerment, and teamwork. The organization emphasizing cooperativeness is typically a friendly place where its members share information and trust one another just like an extended family (Ernest Chang and Lin, 2007).

Furthermore, according to Di Stefano et al. (2019) this type of organization emphasizes teamwork, employee involvement, empowerment, cohesion, and participation; it is held together by loyalty and tradition. On the other hand, shame refers to a feeling of guilt or embarrassment if others know of one’s socially undesirable actions (Vance et al., 2020). The hypothesis asserts that a cooperativeness culture strengthens the positive effect between shame and compliance intention. Siponen et al. (2010) have also hypothesized that shame has an effect on ISP violations within an organization. Therefore, if non-compliance with ISPs is considered breaking norms in the group, we can say that shame has a more substantial impact on cooperativeness culture to deter ISP non-compliance (Di Stefano et al., 2019; D'arcy & Herath, 2011; Siponen et al., 2010). Several factors support this assertion:

Firstly, cooperativeness culture, characterized by cooperation, information sharing, and teamwork, fosters an environment where individuals are encouraged to support one another and work collaboratively towards common goals. Within such a culture, individuals are more likely to experience shame as a result of social disapproval for non-compliance. However, the emphasis on mutual support and cooperation mitigates the negative effects of shame by providing individuals with a supportive network to address their shortcomings and encourage compliance. Consequently, within a cooperativeness culture, the positive effect of shame on compliance intention is strengthened as individuals are motivated to comply in order to maintain the trust and support of their peers.

Secondly, cooperativeness culture promotes open communication and information sharing among its members, fostering an environment of transparency and trust. When individuals experience shame for non-compliance, they are more likely to seek guidance and support from others within a cooperativeness culture. The willingness of individuals to share information and offer assistance facilitates the process of addressing the root causes of non-compliance and finding solutions collaboratively. As a result, within a cooperativeness culture, the positive effect of shame on compliance intention is enhanced as individuals are empowered to overcome their shortcomings with the help of their peers.

Thirdly, cooperativeness culture cultivates trust and empowerment among its members, creating a supportive environment where individuals feel valued and empowered to take ownership of their actions. When individuals experience shame for non-compliance, they are more likely to perceive compliance as a means of restoring trust and reclaiming their sense of empowerment within a cooperativeness culture. The trust and empowerment afforded to individuals within such cultures serve as motivating factors for compliance, strengthening the positive effect of shame on compliance intention.

Moreover, cooperativeness culture emphasizes teamwork and collective responsibility, encouraging individuals to work together towards shared objectives. When individuals experience shame for non-compliance, they are more likely to recognize the impact of their actions on the collective well-being of the team or organization within a cooperativeness culture. The emphasis on collective responsibility motivates individuals to comply in order to uphold the

values of teamwork and cooperation, thus strengthening the positive effect of shame on compliance intentions.

Furthermore, cooperativeness culture provides a supportive environment for personal growth and development, where individuals are encouraged to learn from their mistakes and strive for continuous improvement. When individuals experience shame for non-compliance, they are more likely to view compliance as an opportunity for self-reflection and growth within a cooperativeness culture. The supportive feedback and encouragement offered by peers facilitate the process of learning from past mistakes and making positive changes towards compliance. Consequently, within a cooperativeness culture, the positive effect of shame on compliance intention is magnified as individuals are motivated to seize the opportunity for personal growth and development.

In conclusion, the hypothesis suggests that within a cooperativeness culture characterized by cooperation, information sharing, trust, empowerment, and teamwork, shame exerts a stronger positive influence on compliance intention due to the emphasis on mutual support and cooperation, facilitation of open communication and information sharing, promotion of trust and empowerment, encouragement of teamwork and collective responsibility, and a supportive environment for personal growth and development. These factors collectively contribute to the heightened impact of shame on compliance intentions within the context of a cooperativeness culture. Thus, we propose the following hypothesis:

H11: Cooperativeness culture strengthens the positive effect between shame and compliance intention

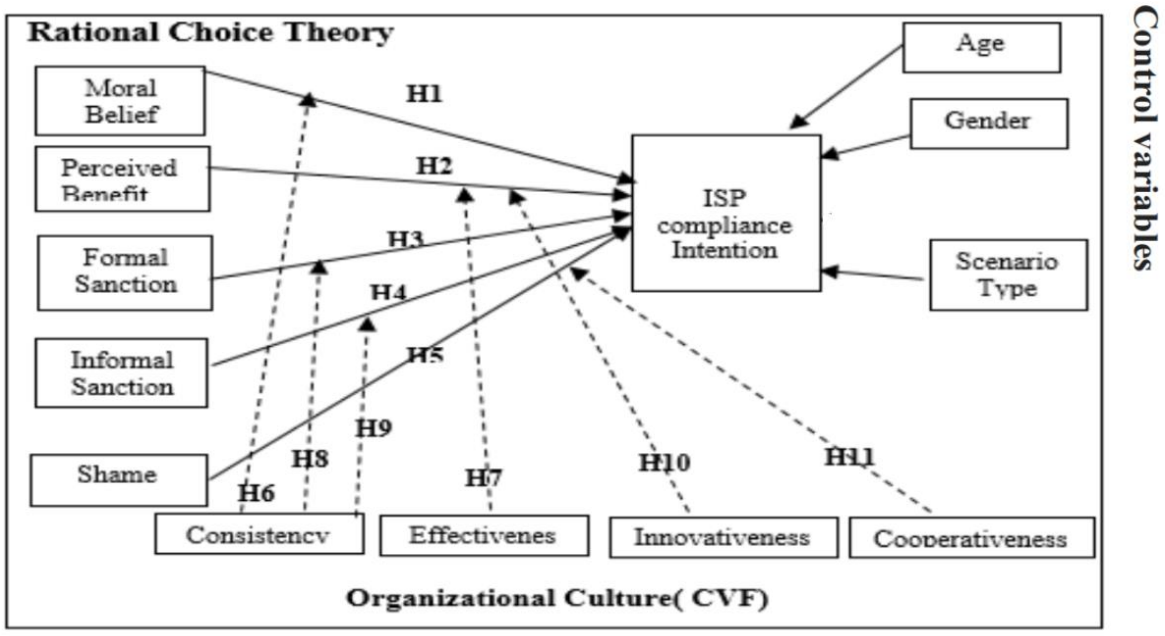


Figure 2. 4 The Research Model

Moderating Role of Organizational Culture Constructs

Organizational culture (OC), conceptualized using the Competing Values Framework (CVF), plays a critical moderating role in shaping employees' behavioral responses to various motivational drivers. In this study, we hypothesize that the four OC dimensions—consistency, cooperativeness, innovativeness, and effectiveness—moderate the influence of RCT constructs on ISP compliance intentions. The following rationale explains the expected moderation effects:

Consistency Culture × Formal Sanctions: A culture that emphasizes rules and stability (consistency) is likely to reinforce the salience of formal sanctions. In such environments, rules are respected and compliance is expected, hence formal sanctions are more likely to deter violations (Cameron & Quinn, 2011).

Consistency Culture × Moral Beliefs: In rule-bound cultures, moral norms are often institutionalized. Employees in such cultures may internalize moral beliefs more deeply, amplifying their effect on compliance intentions (Leidner & Kayworth, 2006).

Cooperativeness Culture × Shame: In cooperative environments, individuals value social harmony and peer perception. Therefore, the anticipation of shame (a social emotion) is expected to be more influential when the culture emphasizes group cohesion (Schein, 2004).

Innovativeness Culture × Perceived Benefits: Cultures that value innovation and flexibility may heighten individuals' perception of the utility of ISP compliance if it aligns with efficiency, innovation, or competitive advantage (Iivari & Huisman, 2007).

Effectiveness Culture × Perceived Benefits: In performance-oriented cultures, the perceived benefits of compliance (e.g., efficiency, protection of assets) are likely to be more influential in guiding behavior (Quinn & Rohrbaugh, 1983).

These relationships are tested empirically through interaction effects in the structural model using PLS-SEM.

2.11. SUMMARY

In this chapter, we have undertaken a careful examination of the extensive body of literature relevant to our research topic, aiming to provide a comprehensive understanding of the landscape surrounding ISP compliance. Our endeavor in this review is twofold: firstly, to cast a revealing light on the existing gaps within the field, pinpointing those that resonate most profoundly with the objectives of our study.

Secondly, we aim to highlight certain fissures that hold broader implications for the field of information security research, thus extending the scope of our inquiry beyond its immediate confines. Drawing upon a diverse selection of disciplines, we meticulously distill the essence of our findings into a set of hypotheses, each poised to unravel key aspects of the phenomenon under investigation. As we transition into the subsequent chapter, our focus shifts towards a meticulous exposition of our research methodology. Here, we unveil the intricate framework that underpins our investigative approach, outlining the strategies and tools we employ to rigorously probe and validate our hypotheses, thereby laying a robust foundation for our empirical inquiry.

CHAPTER THREE: RESEARCH METHDOLOGY

3.1 Introduction

This section explains the methodology used to address the study questions and test the hypotheses formulated in chapter 2. Specifically, it discusses the research philosophy that guides this research, the methods and techniques used in developing research instruments, sample design, data collection procedures, including treatment of the data, and the data analysis approaches used. Finally, it summarizes the chapter and provides a brief description of what is covered in the next chapter.

3.2 Research Paradigm and Method of Study

To establish our observations and reasoning in all types of research works, whatever the purpose of the research, we use our mental models or frames of reference. Paradigms are the names given to such mental frames or models (Bhattacherjee, 2012). Therefore, in research, a paradigm is a philosophical framework that helps guide the scientific research implementation (Collin and Hussy, 2009; Waziri and Kyari, 2023). According to Myers and Klein (2011), a research paradigm is a scheme that consists of assumptions and philosophies about the physical and social world and how to acquire knowledge about it.

Generally, behind the philosophical assumptions of research paradigms, there are two fundamental questions that need to be addressed. The first is the nature of the reality from which knowledge is derived, which is ontology. The second is how to access this reality, that is epistemology (Aliyu et al., 2015; Bhattacherjee, 2012). Ontology is about our assumptions about how we observe the world. This means that ontology deals with the nature of reality, from which knowledge is derived. On the other hand, epistemology is about our assumptions regarding the most effective way to examine the world (Aliyu et al., 2015; Bhattacherjee, 2012). In other words, epistemological assumptions, which guide the methodology of the study, are mainly interested in the practical way of accessing that reality, whereas ontology explains the researchers' views, claims about the nature of reality. It particularly focuses on whether this reality is objective reality or subjective reality, which is created in the researcher's mind (Aliyu et al., 2015; Bhattacherjee, 2012).

Over the years, in their effort to organize their understanding of an inquiry into social life, social scientists have utilized a number of paradigms. When it comes to information system research, the research communities in IS use the popular three research paradigms, namely, the positivist, interpretive, and critical paradigms (Mingers, 2001). On the ontological level, the positivist view of the world accepts that knowledge is quantifiable and objective. The positivist paradigm mainly focuses on measuring phenomena as it occurs in reality, while the interpretive paradigm fundamentally focuses on understanding the phenomenon under investigation from human participants' perspective (Aliyu et al., 2015; Bhattacherjee, 2012). Critical research "attempts to uncover and critique the restrictive and alienating conditions of the status quo by analyzing the oppositions, conflicts, and contradictions in contemporary society and seeks to eliminate the causes of alienation and domination" (Aliyu et al., 2015; Bhattacherjee, 2012).

One of the paradigms that appears to be relevant to this study is positivism. In the positivist view, science is seen as the way to get at the truth and to understand the world in order to predict and control it. According to Bhattacherjee (2012), social reality can be observed and sensed in the physical world, where the researcher is independent of reality. Positivists believe in empiricism, the idea that observation and measurement are at the core of scientific endeavor (Bhattacherjee, 2012).

Different paradigms employ different methodologies, with three major categories being quantitative, qualitative, and mixed methods. Quantitative research reduces data into numbers and uses theories and numerical analysis to reach conclusions. The objective of quantitative research is to build and test models and hypotheses, and it can be designed to be descriptive, showing the association between variables, or it can be experimental, establishing causality between variables (Bhattacherjee, 2012). In contrast, qualitative studies look into non-numeric data, such as descriptions of words, definitions, meanings, characteristics, symbols, and concepts. While quantitative research treats experiences as similar, countable, measurable, or quantifiable (Bhattacherjee, 2012).

Positivists employ the deductive strategy to achieve results in their inquiry, where the researcher begins with a model, theory, or hypothesis, and then collects data to test the theory or hypothesis. Interpretivists, on the other hand, employ the inductive strategy, where the researcher begins

with data collection and then formulates a theory (Gichuru, 2017). Therefore, a quantitative research approach is believed to be appropriate for the present study. The following are the main reasons for considering quantitative research as an appropriate approach to the present study. First, this research work assumes that a phenomenon such as organizational culture and information systems security is a reality that exists in a social world. Thus, ontologically, the objectivism or positivist paradigm matches the assumptions that this study has about reality (Clark et al., 2021).

Therefore, this study intends to empirically investigate the individual variables that predict the behavior of the employee in complying with the ISPs. It aims to understand the factors that predict information security behavior. In doing so, it draws constructs from theories that explain individual behavior and supplements these theories with additional variables to develop a theoretical framework that would be more tailored to explain the phenomenon under investigation. The study considers companies in Ethiopia and deductively generates hypotheses, as well as develops the research model, from relevant theories in the domain. RCT has been used by a number of information systems scholars and has shown clear and sufficient rigorous evidence for explanatory capacity (Kuppusamy et al., 2022), although not in the Ethiopian context.

In general, researchers develop theories through either interpretive/inductive or positivist/ deductive approaches. As this research is in the positivist paradigm, it is imperative to execute positivist prescriptions. Deductive reasoning begins with a general assertion and proceeds to apply that assertion to explain a phenomenon. To draw logical conclusions from premises and ensure absolute certainty, a strict logic of deductive reasoning should be followed (Mueller & Urbach, 2013) after identifying a priori knowledge or theory (Handfield and Melnyk, 1998). An appropriate theoretical base, mainly RCT and CVF, is identified to develop the conceptual model.

The second reason relates to the recognition of the dominance of the positivistic view in information systems research. Arnott and Gao (2022) mentioned that 81% of information systems research was positivist in nature. The quantitative approach is observed as a research tradition of published empirical studies in the domain (Togia and Malliari, 2017).

The third reason relates to the type of data that suits the positivist approach to research. The survey method is employed with the intent of providing objective and numeric data (Opoku et al., 2016; Rashid et al., 2021), through a structured survey instrument, from employees of various organizations in Ethiopia. Hence, it is essential to use a survey method to explain and confirm a set of factors and causal relationships that influence the behavior of employees within the organizational context. The survey method allows the gathering of required data from many participants in remote sites, especially from regional companies in Ethiopia; to make the findings more generalizable while analyzing multiple variables; and to ask many questions and have considerable flexibility in the analysis. Overall, in positivist studies, survey methods are the main data collection methods (Rahi, 2017). Based on the above justifications, as it suits the nature of the current study, the positivist paradigm is a pertinent base for this study.

As a final point, the methodology used in this research is a quantitative method. According to Creswell and Creswell (2017), quantitative studies in earlier times mainly focused on true experiments, correlational studies, and single subject experiments. However, in recent times, quantitative studies have shifted towards more complex experiments with many variables and treatments, including SEM, which involves causal path analysis and investigation of the collective impact of many variables (Creswell and Creswell, 2017). The rationale for adopting a quantitative method is that it provides the ability to produce objective, quantifiable, and reliable data that can be generalized to a larger population. Whenever the purpose of a study is hypothesis testing, quantitative survey research is the most appropriate approach (Creswell and Creswell, 2017).

3.3 Paradigms of Information Security

Researchers are advised to possess a thorough understanding of the conceptual basis of various security methodologies (Bulgurcu et al., 2010). This understanding enables researchers to effectively and methodically apply various security approaches. Scholars suggest different sociological paradigms to aid researchers in recognizing the conceptual foundation of their studies. Burrell et al. (1979) suggest four paradigms: functionalist, interpretive, radical humanist, and radical structuralist. On the other hand, Chua (1986) proposes three research paradigms:

positivism, interpretivism, and critical. The Burrell et al. (1979) sociological paradigm has been extensively utilized in the literature.

However, certain theorists have expressed criticism towards it (Tilahun and Tibebe, 2017). Dhillon and Backhouse (2001) conducted a thorough literature review in the field of information security studies, using Burrell et al. (1979) framework as a basis. Their goal was to gain a conceptual understanding of the various studies in this field. They classified these studies into four quadrants, as described by McFadzean et al. (2006). Thus, this section discusses the essential attributes of two paradigms proposed by Burrell et al. (1979) and provides a rationale for selecting a specific paradigm for this research.

Information security is increasingly becoming more important because of the expanding reliance on digital technologies. Information security helps organizations protect their data integrity and availability (Farayola et al., 2024). Additionally, as stated in the introduction and literature review sections, there is an increasing demand for adherence to regulatory standards in response to threats (Hwang et al., 2017). Hence, various methodologies have been developed to aid security managers in protecting their organizations digital environments from security risks (Soomro et al., 2016). Upon examining the existing literature in the field of information security, it becomes evident that there are two main approaches: technical and non-technical or socio-technical (Malatji et al., 2020). Nevertheless, it is important to mention that scholars, such as Dhillion and Backhouse (2001), consider the terms socio-technical and socio-organizational to be interchangeable (Holgate et al., 2012). In this research, we use these terms without any distinction.

Multiple studies in the literature on information security have demonstrated that the technical approach predominantly emphasizes technology and processes, while disregarding social, organizational, and human factors (Tilahun and Tibebe, 2017). However, despite this limitation, numerous researchers persist in examining information security issues exclusively from a technical standpoint (Ameri, 2023). However, the constraints of the technical approach have led researchers to embrace the socio-organizational approach recommended by Dhillon and Backhouse (2001). While scholars are increasingly agreeing to transition from a focus on technical aspects to a socio-organizational viewpoint, there remains uncertainty regarding the

precise definition of the term "social" within the context of socio-organizational. This is due to the fact that different fields of study have their own unique methods of comprehending and assessing social interactions (Holgate et al., 2012), suggesting that there might be diverse viewpoints on "how to examine socio-organizational issues?" Researchers employ various sociological perspectives to tackle social issues.

Researchers in the field of information security have utilized different methods to tackle social and organizational issues. For example, Dhillon and Backhouse (2001) utilized an interpretive methodology in their research, whereas Foley and Rooney (2019) studied social constructionism in security protocols, considering human experience, psychology, and security. Similarly, Holgate et al. (2012) chose to adopt the perspective of social constructionism. On the other hand, Kam and Katerattanakul (2014) examined, using the neo-institutional approach, how the three external expectations: regulative, normative, and cognitive drive the higher education of the United States to attain information security. Likewise, Hu et al. (2007) employed the sociological neo-institutional approach to examine how institutional factors affect organizational behavior, utilizing a positivist case study methodology. Dols and Silvius (2010) employed the functionalist positivist methodology to investigate the influence of national culture on employees' non-compliance behavior. These studies illustrate how the functionalist paradigm can extend beyond a solely technical viewpoint to include social concerns.

The positivist approach, which falls under the functionalist paradigm, relies on accurately defining facts and quantifying outcomes (Park et al., 2020). Besides, researchers suggested that positivist studies have the same viewpoint, asserting that their purpose is to examine theories and enhance our knowledge of phenomena (Park et al., 2020). Our research supports this approach by initially conducting a comprehensive qualitative literature review of theories pertaining to individuals' compliance behavior with ISPs. Subsequently, we construct a model grounded in these theories to empirically examine multiple hypotheses. Hence, we deem the functionalist positivist approach appropriate for examining how social factors, particularly organizational culture, influence employees' compliance with information security policy.

3.3.1 The Functionalist perspective

There are two main approaches within the functionalist paradigm. The first is the technical approach, which focuses on using checklists, risk analysis, and evaluation. The second is the socio-organizational approach, which uses social theory to study information security issues (Brazevich et al., 2020; Dhillon and Backhouse, 2001). Our discussion will center on the two primary paradigms in the field: positivist and interpretive paradigms.

Burrel and Morgan researchers concentrate on examining the necessity of governing human interactions, a crucial component of comprehensive information security. The primary inquiry that these researchers aim to address is understanding society as a system, a cohesive entity, and an organized structure (Dhillon and Backhouse, 2001). Many aspects of information security are studied within the framework of functionalist paradigm. Many researchers in the field of information security have concentrated on implementing a functionalist structured approach. This approach involves using policies, guidelines, standards, and frameworks to create a secure and stable digital environment. Various techniques such as checklists, risk analysis approaches, and evaluation methodologies are used to achieve this goal (Brazevich et al., 2020).

Checklists are utilized to ascertain all conceivable alternatives for monitoring information. The objective of this technique is to comprehensively analyzes all aspects of a system's security in order to create an "ideal" and impervious system (Baskerville, 1993). Another classification within the functionalist paradigm is the risk category. The risk analysis system is a crucial tool for ensuring information security, as it effectively structures and organizes the entire process, thereby enhancing the development and reliability of the organization's protection system (Brazevich et al., 2020).

A person is a crucial determinant of the system's reliability. Without human control, no automated system, regardless of its apparent perfection, can operate effectively. The management of information and the associated practices of information security and risk reduction are of particular importance. From a risk management perspective, information management plays a crucial role in influencing an individual's response to an abnormal situation that is perceived as a threat to information security. Ongoing research is being conducted in this field (Brazevich et al., 2020).

Functionalist research also encompasses the examination of security policies. In an effort to develop the idea of safeguarding privacy through information security, they suggested several alternatives for these types of systems. Van den Hoven regards privacy as a fundamental human entitlement, with the purpose of safeguarding the inherent worth of individuals (Pieters, 2017). For instance, Kolokotronis et al. (2002) team proposed a complex model that includes multiple levels and dimensions. This model involves analyzing and verifying the organization's needs, studying risks and evaluating their costs, developing a security strategy, and monitoring the outcomes of the strategy (Kolokotronis et al., 2002).

Researchers stress the importance of giving special attention to the issue of information security at the highest level of an organization's management. It should not be seen as a private technical task or a set of tasks solely focused on solving specific problems. Scientists and practitioners have observed a shift in attitude towards the issue of information security. They now recognize that it is not just about software and hardware, but also a significant socio-cultural problem of our time. Ignoring this problem can have catastrophic consequences for society.

Functionalists determined that the environments of different organizations share similar characteristics with the physical world when examining the issue of information security. This enabled them to establish a scientific basis for the concept of information security and management. Functionalists have also concluded that if all subsystems operate efficiently, the organization is effectively shielded from security risks. Therefore, overall security can be guaranteed by thoroughly analyzing the operational methods of the different components of the system. This paradigm has been examined by researchers such as Siponen (2000), Von Solms and Von Solms (2005), and Vorster and Labuschagne (2006), as referenced in Njenga and Brown (2008).

3.3.2 The interpretive perspective

The interpretive perspective refers to a specific approach or viewpoint used to analyses and understand a particular subject or phenomenon. Cardoso and Ramos (2012) explain that the interpretive paradigm provides a different viewpoint compared to the functionalist paradigm. This approach posits that knowledge is acquired through social constructions. Although the interpretive approach offers certain benefits, such as offering an in-depth understanding of the

problem domain, it also has drawbacks, such as its complexity resulting from its intricate philosophical and sociological foundations. In the past, the functionalist approach was prevalent in information security studies, but there has been an increasing fascination with the interpretive paradigm in recent decades (Brazevich et al., 2020). Nevertheless, the majority of efforts to employ this paradigm have concentrated on conventional information security disciplines while disregarding information system domains.

In the 1990s, numerous strategies for overseeing information security heavily relied on computer science and database management techniques, neglecting the human factor. Nevertheless, there was an increasing inclination to take into account the socio-technical dimension of information security management, as evidenced by the scholarly contributions of (Dhillon and Backhouse, 2001; Dzazali et al., 2009; Waly, 2013) and other researchers.

Dhillon and Backhouse (2001) argued that the majority of strategies for managing information security rely on the metaphor of the 'organization as a machine' and fail to consider the human factor. In the 1990s, there was an increasing inclination in the field to acknowledge the socio-technical dimension of information security management, despite its limited and isolated status during that period. Willcocks and Margetts (1994) determined that social and qualitative factors are crucial in the analysis of risks in information systems security. D. W. Straub and Welke (1998) employed the interpretive paradigm to formulate recommendations for safeguarding information system against security breaches. Baskerville previously concentrated on employing structured and mechanistic methodologies for information security. However, he has recently demonstrated a keen interest in utilizing the interpretive approach, particularly in the context of risk analysis for information security design. Several researchers, such as Dobson (1991) and Stren and Dobson (1993), utilize conventional interpretive social theories to comprehend information security issues. In addition, M. T. Siponen (2001) observed that numerous information security management approaches at that time heavily depended on techniques and methods derived from computer science and database management systems.

3.4 Research Design

The research design for this study involved the use of the theoretical scenario method to evaluate how respondents intend to comply with ISP regulations. The scenario method was chosen for its potential benefits in the area of ISP compliance and non-compliance. The research design issues that were addressed in the following subsections include why the scenario method was chosen, how the scenarios were developed, the pre-test procedure, and the overall process of instrument development.

3.4.1 Scenario Method

The scenario method used in this study provides a clear and realistic description of a situation or phenomenon, and respondents rate their answers on a scale that measures the dependent variable. Compared to the traditional survey method, which asks general questions, the scenario method offers several advantages (M. Siponen and Vance, 2014; Vance et al., 2020).

For instance, Pogarsky and Piquero (2004) suggest that the scenario method is a suitable way to examine ethical and unethical behavior, as it provides an indirect approach to measuring individuals' intention to engage in socially undesirable actions, which can be challenging to measure using conventional surveys. This is because people may conceal their true intentions and provide socially acceptable responses. Moreover, as the scenario method presents a hypothetical third-party situation, respondents may be more willing to express their support for the person's behavior. As ISP noncompliance is considered socially undesirable, the scenario method is more appropriate than conventional surveys.

We selected this approach due to its widespread use in ISP compliance research (M. Siponen and Vance, 2014; Vance et al., 2020). As a result, our research can be considered similar to many previous studies. Another advantage of the scenario method is its ability to measure socially undesirable behaviors in a prospective manner because the scenario method offers a less threatening approach to assessing ISP intentions compared to directly asking employees to self-report their own breaches. Furthermore, traditional survey methods are limited to measuring past behavior with current perceptions of constructs in the survey. Therefore, when conducting surveys on ethical dilemmas, it is preferable to use prospective measures of behavior such as "intention to commit an act." Moreover, scenarios offer a means to enhance generalizability by

integrating diverse situations into multiple scenarios (Barlow et al., 2013; M. Siponen and Vance, 2010; Vance et al., 2020).

3.4.2 Scenario Design

Ensuring an accurate representation of important and commonly encountered information security concerns holds the greatest significance in the steps of scenario design. Vance and Siponen (2012) state that a crucial element in the design of scenarios is the necessity of ensuring their realism and familiarity with participants. In order to enhance the validity and realism of our scenarios, we conducted interviews with information security officers from five organizations in Ethiopia and seven organizations in Finland. According to Vance and Siponen (2012), researchers have proposed various approaches for designing scenarios that are practically relevant in the context of employees' ISP compliance. According to Vance and Siponen (2012), researchers have proposed various approaches for designing scenarios that are practically relevant in the context of employees' ISP compliance.

The first approach involves conducting a thorough examination of the existing literature in order to compile a comprehensive inventory of statements pertaining to compliance or violation of information security policy. These statements are subsequently assessed and prioritized by information security officers, taking into account their relevance to the research objectives. The second methodology entails the development of diverse scenarios, wherein information security officers are requested to assess, provide commentary on, and assign a ranking to their relevance. The third approach involves asking for input from information security officers to ascertain the dominant and relevant instances of noncompliance or violations pertaining to information security policy. According to Vance and Siponen (2012), the initial approach primarily centers on the verification and ranking of pre-existing knowledge. In contrast, the latter two approaches afford researchers the opportunity to acquire novel perspectives on noncompliance or violations within the context of information security policy. Consequently, the third approach was employed in our study to generate contemporary, prevalent, and suitable scenarios (Vance et al., 2020).

During the survey development , information security officers were asked to identify the five most prominent scenarios of compliance problems related to information security policy that

commonly arise within their respective organizations. The most frequently reported security concerns were classified into ten distinct categories based on the participants' responses. The observed behaviors encompassed various infractions, such as sharing customer information, password sharing, failure to report computer viruses, leaving computers logged in and unattended, writing passwords in visible locations, using the internet for non-work activities, playing games during work hours, failure to update antivirus software in a timely manner, and using personal flash disks without scanning for viruses.

We then asked information security officers to rank the top five relevant ISP noncompliance or violations, and the majority (90%) voted for password sharing, leaving computers logged in and unattended, and sharing customer information. We included a variety of scenarios in our research to ensure comprehensive coverage and improve the generalizability of our findings.

Afterwards, we proceed with the formulation of the scenarios for the five aforementioned cases. According to Arage et al. (2015), when formulating scenarios, various factors must be considered, like the inclusion of specific details such as individuals' names, and the scenarios should address prevalent and significant security concerns. The scenarios utilized in this study include writing passwords in visible locations and sharing them; neglecting to log out of workstations; sharing customer information without proper authorization; using personal flash discs without scanning them with antivirus software; and failing to report computer viruses. These scenarios were derived from the works of (Arage et al., 2015; Ernest Chang and Lin, 2007; Moody et al., 2018; M. Siponen et al., 2010; M. Siponen et al., 2012; Vance and Siponen, 2012(Ernest Chang, 2007 #320)). After receiving feedback from language editors and information security officers, the design of these hypothetical scenarios has been completed. The next section will provide further details on the hypothetical scenario that has been selected.

Password sharing

Casey splits her time working in the offices of two different degree programs offered at the university. In one of the offices, she is responsible for tracking the current status of research grant funding allocations for the entire department; this information is accessed using a special program that is only loaded on her office computer hard drive. Casey is aware of the university's policy that each computer workstation must be password protected and that passwords are not to

be shared. However, since Casey moves between job locations regularly, she shared the password to her office computer with several coworkers so that they can get the information they need when they need it. Casey expects that sharing her password will save her coworkers a lot of time and effort instead of waiting for her to get back to the office (Moody et al., 2018; M. Siponen and Vance, 2010).

Workstation logout

Jordan works in the front office of a popular degree program offered at the university. His duties require frequent interaction with faculty, staff, students, and outside clients both at and away from his desk. Jordan is aware of the university's policy that employees must log out of or lock their computer workstation when not using it. When Jordan knows or believes he is going to be away from his desk for an extended period of time (one hour or longer), he locks his computer. However, based upon his typical schedule of frequent departures to and from his desk, Jordan mostly keeps his user account logged-in to save him time in performing his normal duties (Moody et al., 2018; M. Siponen and Vance, 2010).

Sharing customer information

Jack is working in a position that requires access to his company customers' personal information. His company's information security policy prohibit him from giving the customer's personal information detail to anyone, except the main office. Jack is expected to send some of the customers' personal information to the main office but the internet connection in his office is too slow to send the data. Therefore, Jack believes that asking his friend to send the customer information from his office with a convenient internet connection could save a lot time and money for the company. He also know that an employee was recently reprimanded for sending the data through unauthorized person. Jack gives the data to his friend so that he will send it to the main office (Arage et al., 2015).

USB drive

Pekka is a middle level manager in a medium-sized company where he has worked for several years. Pekka is currently working on a sales report that requires the analysis of the company's

customer database. This database contains customer names, phone numbers, credit card numbers, and purchase histories. Because of the sensitive nature of corporate data, the company has a strict policy prohibiting the copy of corporate data to unencrypted portable media, such as USB drives. However, Pekka will be traveling for several days and would like to analyze the corporate database on the road. Pekka expects that copying the data to the USB drive and taking it on the road could save the company a lot of time and money. The firm is experiencing growing sales and revenues in an industry that is economically deteriorating. He also knows that an employee was recently reprimanded for copying sensitive corporate data to a USB drive. Pekka copies the corporate database to his portable USB drive and takes it off company premises (M. Siponen and Vance, 2010).

Failing to report computer virus

Gina is browsing possible questionable websites at work and the anti-virus program alerts her that a virus has been installed on her computer. Although the information security policy requires that IT support staff remove viruses, Gina decides to take care of the virus problem by herself (Vance et al., 2012).

3.4.5 Instrument Development

Paying close attention to instrumentation can help clarify the interpretation of research questions, as highlighted by MacKenzie et al. (2011). The questions in a survey instrument should measure the intended concepts or behaviors, accurately reflect the true values for the measures, and minimize random variability while being sensitive enough to detect meaningful differences or changes and covering all dimensions of the topic being investigated, as stated by Collins (2003).

We utilized previously validated instruments from (Arage et al., 2015; Ernest Chang and Lin, 2007; Moody et al., 2018; M. Siponen et al., 2010; M. Siponen et al., 2012; Vance and Siponen, 2012(Ernest Chang, 2007 #320)) to operationalize all the constructs. The instrument consists of three sections, each containing six to eight questions. The initial segment of the survey collects demographic information pertaining to the participants, encompassing variables such as gender, educational background, professional experience, and job designation within the organization.

The second section comprises tools specifically developed for evaluating the research variables in RCTs, while the final section encompasses tools designed for assessing the variables related to organizational culture. On average, respondents typically require approximately fifteen minutes to complete all the items.

When providing responses, participants were instructed to indicate the most appropriate option on the provided scale by circling it. The interval scale was employed in order to facilitate the computation of specific arithmetic operations based on the gathered data. The researcher employed a 5-point Likert scale as the method of scaling. The Likert scale is a measurement tool that is specifically designed to assess the degree of agreement or disagreement among participants in relation to statements, utilizing a five-point scale (Cavana et al., 2001). Please refer to the sample questionnaire provided in Appendix I. Further details on the operationalization of each of the theoretical constructs are discussed below.

As a component of our investigation, we account for control variables, such as age, gender, and scenario type, along with dependent, independent, and moderator variables. Past research indicates that these elements can influence whether an individual intends to follow or disobey their organizational ISP. Age and gender have been shown to have an effect on information security misuse intention (Leonard and Cronan 2001; Leonard et al. 2004). Additionally, we incorporate scenario type as a control variable, as we randomly allocate each respondent one of five scenarios (Vance and Siponen, 2012).

3.4.6 Pilot testing

The pre-test is an important step in the research process after finalizing the survey instrument. Its purpose is to ensure that the survey instrument functions as a reliable and valid research tool. According to Converse and Presser (1986), pretesting helps researchers ensure that the survey items are accurately described, and the response options are complete, important, and mutually exclusive. It also ensures that both the researchers and respondents understand the instruments in the same way, helping researchers correct vague terminologies, unfamiliar references, and ambiguous words and phrases. Additionally, pretesting enables researchers to evaluate response latency, which is the time taken to complete each item and the whole survey. (Bassili and Scott, 1996).

According to Jansen and Hak (2005), when conducting a pertest on survey items, experts should be asked to rate individual questions on a Likert scale. The purpose is not to gather expert opinions and beliefs, but to evaluate how well the survey items reflect the construct being measured. In our pre-test, we engaged a group of information security experts to review our survey instruments and scenarios, and ensure they had strong content validity (Lewis et al., 2005). We selected 30 experts from Ethiopia and Finland, including 8 practitioners and 22 academicians, to provide a broad range of perspectives. We found the practitioners' feedback on the scenarios to be particularly valuable due to their experience with different types of ISP compliance and noncompliance. Based on their input, we made some minor improvements to the scenarios, such as clarifying the context in which information security compliance occur and using simpler language. The final hypothetical scenarios have been included in Appendix I. Overall, the experts agreed that the five scenarios covered common ISP compliance issues, which helped ensure that respondents would be familiar with the scenarios. Sheatsley (1983) recommends selecting between 12 and 50 experts for a pre-test, and we believe our sample size of 30 provided a sufficient range of perspectives.

The academicians' feedback on the survey instrument items was instrumental, covering aspects such as question flow, instrument measurement quality, and item wording. In response, we made modifications to the survey layout by rearranging the questions to ensure a logical and intuitive sequence. We also improved the scenario-related questions' placement by positioning them directly after the scenarios and placing the organizational cultural questions in appropriate places. Additionally, we revised some item statements to replace general references with specific names, like Jack. Based on this constructive feedback, we updated the survey instruments accordingly. As Olson (2010) suggests, a logical and intuitive survey instrument layout can reduce respondents' burden and improve data quality.

Then next, we conducted a pre-test survey on a small subsample of the population to improve the questionnaire. Pretesting helps researchers to ensure that the survey questions are clear and appropriate for the cultural and demographic profile of the larger sample (Ferketich et al., 1993). We distributed the questionnaire to 37 employees in Ethiopia and asked for their feedback on issues such as clarity of questions and instructions, practical problems faced during questionnaire

completion, and time taken to complete the questionnaire. After sending reminder emails to non-respondents, we received twenty six (76%) usable responses. All respondents reported that the questions and instructions were clear and easy to understand, except for a minor comment on the use of an abbreviation, which we corrected, and some order to the questions. Respondents also provided feedback on the amount of time required to complete the questionnaire. Although our initial assumption was to allocate twenty minutes, the average response time was around fourteen minutes; therefore; we revised the response latency to fifteen minutes to make it more convenient for respondents. Based on the pilot results, we made necessary adjustments to the survey instruments, and the final version of the questionnaire can be found in Appendix I.

3.5 The sampling frame

When conducting empirical quantitative survey research, researchers must take great care to design a sample that accurately reflects the theoretical population. This study's population includes all current Ethiopian employees who work for companies that have ISPs. A method called PLS-SEM was used for the analysis. We think that the number of usable reactions should be at least 200. Table 4.1 shows that there are 553 usable reactions, which is a lot more than the minimum number set by Weston and Gore (2006).

We first selected key cities throughout Ethiopia, followed by selected organizations with the ISP to select potential respondents. Given the lack of a well-documented ISP by many companies in Ethiopia (Yigezu, 2011), it is challenging to have a simple ISP for the few organizations. We managed to get organizations to ISP and communicate with each organization's human resources departments by randomly selecting staff. The following paragraphs illustrate how we handled the final selection process.

In the process of the study, we strived as far as possible to include employees from various cities in the country, so that our respondents would be a greater representation of the Ethiopian national community. In this regard, we first discussed in detail the demographic and cultural situation of Ethiopian regions with those who had detailed knowledge. Accordingly, according to these sociologists, the five cities of Ethiopia are considered representative of Ethiopia's core cultural characteristics. We chose towns, in accordance with their suggestion: the cities with the sampling frame of this study include Addis Ababa, Adama, Bahir Dar, Dire Dawa, Hawassa, and Mekele.

To implement this framework first, organizations in the cities with a well-established information security policy were expected to be identified. During the identification process, important contacts were made with the ministerial offices at the regional and federal level (i.e., the Ministry of Communications and Information Technology, Information Network Security Agency (INSA), and the national, regional offices for the development of ICT in each of these cities), as well as with the various key staff in charge of the coordination of these efforts. After this communication, we will receive a list of organizations around seven hundred organizations that are known or registered by the offices as having an information security policy. As it is not possible to include all such organizations, we have selected representative organizations using the random sampling method (i.e. lottery method), finally choosing the following: city banks and insurance companies, universities in each city, city administration, and offices in some cities.

Thus, our sample framework in Ethiopia covers banking and insurance companies and universities, municipal authorities, and certain Ethiotelecom offices in various parts of the country. By conducting very long and tiresome contact with the human resources department and other interested bodies in each organization, we managed to get permission to meet individual respondents. During our communication with the various offices, we have tried to describe the purpose of research, and we have provided them with a document discussing the issues of research purpose, procedures, risks and benefits, anonymity and confidentiality, reimbursement, freedom to withdraw, responsibility and permission of the subject. Appendix II provides the consent document. In particular, the agencies gave us a list of employees' names, from which we have randomly selected some respondents. The selected sample technique is a random sampling technique. A paper-based questionnaire was submitted to all respondents. The reason behind utilizing a paper-based survey is due to the requirement of internet connectivity and email addresses for each respondent, which poses challenges in meeting these criteria in the context of Ethiopia.

After we handled the participant's questionnaires, we could return the completed questionnaires almost within two months, and we continuously visited the respondents to help us increase the response rate. We obtained 553 usable responses at the end of the data collection process, which means a response rate of 36.8 percent, above minimum demand.

3.6 Demographic Analysis

The data gathered from the respondents' answers to the questionnaire items was utilized to construct profiles of the participants in the survey. These profiles encompassed variables such as age, gender, level of education, and city of residence. Table 4.1.displays the statistical data corresponding to each of these factors for the purpose of examination.

Construct	Items	Frequency	Cumulative Percent
Gender	**1**	355	64.2
	2	198	35.8
Education level	**1**	14	2.5
	2	89	16.1
	3	328	59.3
	4	122	22.1
Scenario types	**1**	117	21.2
	2	111	20.1
	3	102	18.4
	4	110	19.9
	5	113	20.4
Age	Mean	35.92	
	Median	35	

Table 3. 1: Demographic Analysis

Of the total individual respondents that have reported their gender (N=553), 64.2 percent of the respondents are 1 (n=355), and 35.8 percent of the respondents are 2 (n=198). 59.3 percent (n=328) of the respondents had 1, whereas 22.1 percent (n=122) held 4. 16.1 percent (n=89) of the respondents held 2 and 2.5 percent (n=14) of the respondents held 1. The results of scenario types of respondents indicate that 21.2 percent (n=117) are 1, 20.1 percent (n=111) are 2, 18.4

percent (n=102) are 3, 19.9 percent of the respondents are 4 (n=110), and 20.4 percent (n=113) of respondents are 5. The mean age of respondents is 35.92.

3.6.1 Data cleaning

This section presents a description of the procedures that were employed to examine and prepare the data for the intended analysis. While it is widely acknowledged that the PLS method is not reliant on distributional assumptions (Hair et al., 2021; Ringle et al., 2012), it is still necessary to provide some information regarding the distribution of the population from which the data sample was derived. This is done to gain a general understanding of the population's distribution and to demonstrate the appropriateness of the statistical estimation procedure.

3.6.2 Missing data

We conducted a thorough examination of the data to minimize the potential for errors stemming from data entry from the questionnaire. Additionally, we assessed the entire dataset to determine the extent of missing data, both in terms of the number of variables and cases. To ensure data accuracy, we followed the guideline proposed by Hair et al. (2010), which suggests removing cases with more than 10% missing data and variables with more than 15% missing data. We identified 39 cases with more than 5 (11%) missing values across all variables, and these cases were subsequently removed. Most of these instances were due to issues like missing pages or errors in printing and stapling.

Regarding the variables, none of them had missing values exceeding 15%, with the highest being 4%. Consequently, we retained all variables without deletion. The purpose of this analysis was to determine whether the extent of missing data, either per variable or per case, warranted the application of corrective techniques.

Moreover, despite the relatively low prevalence of missing data, we utilized the EM algorithm for imputation purposes, resulting in a complete dataset with replacement values. This approach was chosen to ensure the most accurate estimates from the data, including obtaining valid values for weighted scores, and to prevent any potential unnoticed effects of missing data, as recommended by J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017). This method is believed to handle both random and non-random missing data processes effectively, thereby

offering the closest representation of the original value distribution (J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M., 2017).

3.6.3 Test for Normality

Following the advice of J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017), we looked at the skewness and kurtosis of each indicator to figure out how the final sample data was distributed. It is important to remember that normality of data distribution is not a strict requirement in PLS-SEM. However, checking for skewness and kurtosis is useful because high levels of these can affect the results of the structural model and help you figure out what needs to be done to fix the problem.

In this section, we present the results of the normality analysis. We used skewness and kurtosis to assess the multivariate normal distribution of the data. It's important to remember that PLS-SEM doesn't have to assume that the data is normally distributed. However, looking at skewness and kurtosis can be helpful because they can change the results of the structural model and help you figure out what needs to be done to fix things. The values for asymmetry and kurtosis between -2 and +2 are considered acceptable in order to prove a normal univariate distribution (George and Mallery, 2019). Mean and standard deviation (Cyprian Maphanga and Jokonya) as well as skewness and kurtosis, are shown in Table 4.2. Table 4.2 shows that all of the skewness (ranging from -0.117 to -0.994) and kurtosis (ranging from -1.149 to 1.040) indices were within their acceptable ranges. This suggests that the data is pretty normal. In closing, the results of the tests performed confirm the overall validity of the data for further analysis.

Items	Mean	Std. Deviation	Skewness	Kurtosis
MB_1	3.034	1.212	0.020	-1.009
MB_2	3.061	1.211	-0.063	-1.011
MB_3	2.951	1.205	0.138	-1.046
PBC_1	3.477	1.058	-0.567	-0.352
PBC_2	3.458	1.190	-0.326	-0.887
PBC_3	3.371	1.236	-0.392	-0.877
PBC_4	3.427	1.240	-0.429	-0.878

PBC_5	3.382	1.270	-0.356	-1.031
PBC_6	3.441	1.247	-0.442	-0.866
FSC_1	3.380	0.975	-0.490	-0.259
FSC_2	3.452	1.043	-0.564	-0.287
FSC_3	3.354	1.125	-0.508	-0.610
FSC_4	3.137	1.229	-0.111	-1.112
FSC_5	3.087	1.198	0.042	-1.081
FSC_6	3.061	1.244	-0.003	-1.145
ISC_1	3.553	0.875	-0.937	0.807
ISC_2	3.774	0.937	-0.994	1.040
ISC_3	3.638	1.016	-0.801	0.260
ISC_4	3.609	1.058	-0.718	0.029
ISC_5	3.617	1.011	-0.768	0.269
ISC_6	3.678	1.022	-0.774	0.199
SC_1	3.300	0.978	-0.397	-0.461
SC_2	3.307	1.131	-0.067	-0.988
SC_3	3.405	1.117	-0.308	-0.703
SC_4	3.445	1.150	-0.391	-0.689
SC_5	3.490	1.108	-0.415	-0.595
SC_6	3.490	1.053	-0.445	-0.432
CONS_1	3.345	1.236	-0.356	-0.931
CONS_2	3.212	1.223	-0.100	-1.080
CONS_3	3.382	1.270	-0.564	-0.805
CONS_4	3.286	1.195	-0.278	-0.941
CONS_5	3.213	1.234	-0.296	-1.002
CONS_6	3.354	1.197	-0.417	-0.769
EFFE_1	3.235	1.267	-0.336	-0.999
EFFE_2	3.179	1.261	-0.248	-1.034
EFFE_3	3.081	1.327	-0.117	-1.149

EFFE_4	3.166	1.225	-0.220	-0.967
EFFE_5	3.098	1.283	-0.183	-1.097
EFFE_6	3.141	1.276	-0.224	-1.070
INNO_1	3.617	1.289	-0.736	-0.593
INNO_2	3.568	1.302	-0.644	-0.729
INNO_3	3.438	1.346	-0.587	-0.897
INNO_4	3.503	1.180	-0.641	-0.445
INNO_5	3.445	1.254	-0.582	-0.740
INNO_6	3.508	1.258	-0.517	-0.828
COOP_1	3.552	1.160	-0.653	-0.422
COOP_2	3.562	1.189	-0.603	-0.561
COOP_3	3.546	1.221	-0.662	-0.495
COOP_4	3.499	1.243	-0.575	-0.735
COOP_5	3.524	1.234	-0.542	-0.763
COOP_6	3.655	1.162	-0.754	-0.258
COOP_7	3.609	1.170	-0.742	-0.270
COOP_8	3.647	1.169	-0.755	-0.261
INT_1	3.204	1.048	0.134	-0.829
INT_2	3.098	1.038	0.106	-0.668
INT_3	3.069	1.039	-0.060	-0.726

Table 3. 2: Descriptive Statistics and Normality

3.6.4 Tests for common method bias

Common method bias, "is the variance that cannot be explained by correlations with variables, but is due to unreliability in the data-gathering process" (Joseph F Hair Jr et al., 2021). When a variable is more highly correlated with one or more variables, the common variance increases. Yet, due to data collection errors, rather than the relationships hypothesized in a given research model, the amount of possible common variance can be reduced. This could be a result of the data collection method allowing for all data to be self- reported, collected through the

same instrument. This makes it harder to connect the variable to any other variable in the model (Straub et al., 2004), which leads to systematic measurement error and skewed estimates of the real relationship between the theoretical constructs (Podsakoff et al., 2003).

The most commonly proposed test to identify and diagnose method bias is Harman's single-factor test (Podsakoff et al., 2003). Thus, all 56 variables were entered into an exploratory factor analysis using principal components factor analysis with varimax rotation to determine the number of factors that are necessary to account for the variance in the variables. If a substantial amount of common method variance is present, either (a) a single factor will emerge from the factor analysis or (b) one general factor will account for the majority (>=50%) of the covariance among the variables (Podsakoff et al., 2003).

As indicated in Table 4.3, the percentage of variance accumulated in the first component, is 22.952 percent. This value is well below the cut-off value of 50 percent. Therefore, the results of these analyses do suggest that common method variance is not of great concern and is unlikely to affect the interpretations of results, or simply that the data is free from common method variance effects.

Component	**Initial Eigenvalues**			**Extraction Sums of Squared Loadings**		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	12.853	22.952	22.952	12.853	22.952	**22.952**
2	9.306	16.618	39.569			
3	3.535	6.313	45.882			
4	2.946	5.260	51.143			
5	2.237	3.995	55.137			
6	1.907	3.405	58.542			
7	1.876	3.350	61.891			
8	1.665	2.973	64.864			

9	1.436	2.564	67.428
10	1.067	1.905	69.333

Table 3. 3: Test for common method bias

3.7 Data analysis technique

This study utilizes structural equation modeling with a focus on PLS-SEM version 3 for data analysis. SEM is a robust statistical technique that allows for the examination of complex models and rigorous variance analysis (Andreev et al., 2009; Gefen et al., 2000; Joe F Hair Jr et al., 2017). Unlike traditional first-generation regression models that analyze item loadings and relationships with dependent variables separately, SEM offers several advantages:

In selecting PLS-SEM for data analysis, scholars recommend it over covariance-based structural equation modeling (CB-SEM) for several reasons (Joe F Hair Jr et al., 2017). PLS-SEM is particularly useful when developing theories, especially for predictive and explanatory types of theories. This approach is well-suited for areas with limited empirical descriptive theories, such as information security, which aligns with the objectives of this research.

Another advantage of PLS-SEM is its ability to handle both reflective and formative measures, as well as single-item constructs, without identification problems. Given the complexity of the research model, PLS-SEM's capacity to manage latent variables with formative and reflective measures is crucial. Additionally, PLS-SEM provides greater statistical power, making it attractive for predictive studies (Joe F Hair Jr et al., 2020).

Furthermore, PLS-SEM is known for its efficiency and precision in rendering specific relationships significant in the sample when they are indeed significant in the population, a crucial quality for predictive constructs obtained from cross-sectional sample data and chi-square tests. For the analysis, PLS-SEM V.3 software was used for both exploratory factor analysis and path analysis. SmartPLS has gained popularity in information systems studies (Hubona, 2009). In addition to SmartPLS, Statistical Software for Social Science or SPSS and Microsoft excel are employed for data analysis, with excel primarily used for data entry.

3.7.1 Moderation Analysis Procedure

To assess the moderating role of organizational culture (OC) dimensions on the relationships between Rational Choice Theory (RCT) constructs and ISP compliance intention, moderation analysis was conducted using **Partial Least Squares Structural Equation Modeling (PLS-SEM)** in **SmartPLS 4**.

Following the guidelines of Hair et al. (2021), we used the **product indicator approach** to construct interaction terms. For each hypothesized moderation effect, interaction terms were created between the OC dimension (moderator) and the respective RCT construct (independent variable). All indicators of the latent variables were mean-centered prior to interaction term computation to reduce multicollinearity.

The significance of each interaction effect was assessed by examining the **path coefficient (β)** and **p-value** of the interaction term. A statistically significant interaction indicates that the OC dimension moderates the relationship between the RCT construct and ISP compliance intention. Moderation was further visualized using **simple slope plots** to interpret the nature of the interaction (e.g., amplifying or dampening effect). The interaction terms were also evaluated for **effect size (f^2)** to determine their contribution beyond the direct effects.

3.8 Chapter summary

This chapter extensively examined the range of methodological options available and explicitly outlined those that have been adopted for this research endeavor. Rooted within a positivist paradigm, the research methodology entailed a meticulous process of crafting and refining the instrument design, encompassing the delineation of the construct's scope, item generation, pre-testing, and pilot testing phases. The study's sampling framework was meticulously defined, focusing on Ethiopian institutions, from which a representative sample was drawn. The data collection phase involved physical visits to the selected institutions, affording invaluable firsthand insights gathered through the administration of paper-based surveys. Subsequently, meticulous efforts were undertaken to prepare the collected data for analysis, including

addressing missing data issues from each questionnaire and implementing strategies to mitigate common methods bias. Finally, the chapter elucidated the rationale behind adopting the PLS-SEM method for data analysis, underscoring its suitability for the research objectives at hand.

CHAPTER FOUR: INSTRUMENT VALIDATION AND RESEARCH MODEL ANALYSIS

4.1 Introduction

As emphasized by D. Straub et al. (2004) and Fong and Law (2013) the credibility of any empirical research is established by the degree of data accuracy and the validity of the research instrument used to collect the data. Since measuring theoretical constructs always carries the potential for error, the primary goal of instrument validation is to establish methods for minimizing measurement errors (D. Straub et al., 2004). To assess validity, we followed two influential guidelines: criteria for evaluating partial model structure (J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M., 2014; Urbach and Ahlemann, 2010) and positivistic research validation (D. Straub et al., 2004; Urbach and Ahlemann, 2010). These guidelines have served as the foundation for numerous information security research projects based on PLS.

In order to assess the degree of alignment between the observed data and the theoretical model, the Partial Least Squares method encompasses two distinct analytical stages. The first stage, known as the measurement model, involves evaluating the quality of relationships between the constructs and their corresponding measurement items to assess the overall structure of the model. The second stage, referred to as the structural model, focuses on evaluating the interrelationships among the constructs themselves. Consequently, the process of determining validity in partial least squares is carried out by means of these two distinct phases. The subsequent section of this chapter presents a comprehensive overview of the assessment process for both the measurement and structural models.

4.2 The empirical model

This section discusses the methodologies utilized to establish the validity and reliability of the survey instrument. As emphasized by scholars such as Hair et al. (2014), Ringle et al. (2012), and Hair et al. (2010), validity and reliability are attributes of a measurement tool that enhance the trustworthiness of research findings within the academic community. Validity, as defined by Hair et al. (2010, p. 3), refers to "how accurately a measure or a set of measures truly represents the concept under investigation." Conversely, reliability is described as "the degree to which a

variable or a set of variables consistently measures what it is intended to measure" (Hair et al. 2010, p. 2).

4.3 Assessment of the measurement model

An essential step is included in the assessment of the measurement model in the PLS-SEM analysis. This step involves making certain that the reliability and validity of the measurement model in PLS analyses are maintained. According to Sarstedt et al. (2019) and J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017), it is essential to investigate four critical elements in order to evaluate the measurement model for reflective constructs. These elements are internal consistency reliability, indicator reliability, convergent validity, and discriminant validity. Figure 4.1 presents a visual representation of the measurement model that was used for this investigation.

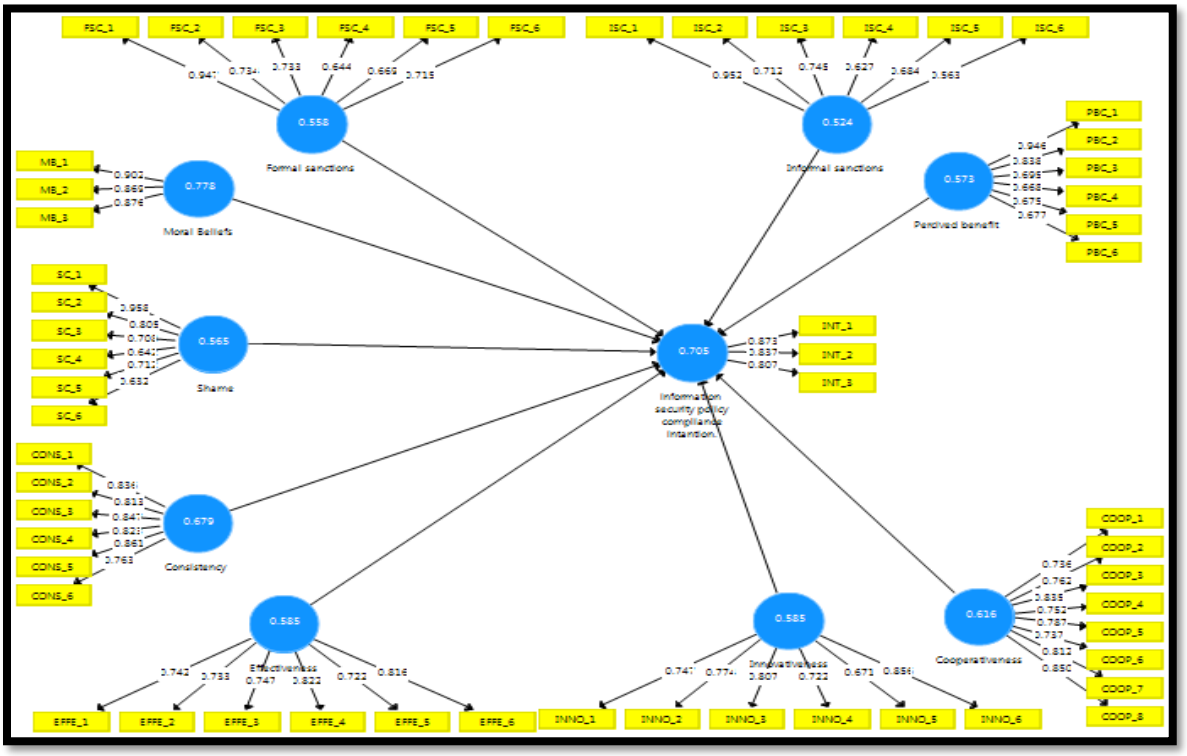


Figure 4. 1: Measurement Model

Among the generally recognized techniques to assess reliability are indicator reliability and internal consistency reliability. In the next subsection, let us start a discussion regarding reliability assessments.

4.3.1 Indicator Reliability

According to Andreev et al. (2009), the assessment of indicator reliability for constructs is accomplished by examining the indicator weights. Indicator reliability is assessed using outer loading values. According to (Hair et al., 2021), outer loadings are the bivariate correlations between a construct and the indicators. The outer loadings for each item should be greater than 0.50 (Chin, 1998). Indicator reliability is the other measure of convergent validity (Hair et al., 2021). If the associated indicators of a construct have much in common, it shows higher convergence. Usually, loading values of items above 0.50 are accepted (Gefen et al., 2000). In this study for the evaluation of the indicator reliability, the cut-off value for loadings of 0.50 is accepted. The results of outer loadings are presented in Figure 4.1 and Table 4.4.

Indicators	**Moral Beliefs**	**Perceived benefit**	**Formal sanctions**	**Informal sanctions**	**Shame**	**Consistency**	**Effectiveness**	**Innovativeness**	**Cooperativeness**	**Intention**
MB_1	0.902									
MB_2	0.869									
MB_3	0.876									
PBC_1		0.946								
PBC_2		0.838								
PBC_3		0.695								
PBC_4		0.668								
PBC_5		0.675								
PBC_6		0.677								
FSC_1			0.947							

FSC_2	0.734				
FSC_3	0.733				
FSC_4	0.644				
FSC_5	0.669				
FSC_6	0.715				
ISC_1		0.952			
ISC_2		0.712			
ISC_3		0.745			
ISC_4		0.627			
ISC_5		0.684			
ISC_6		0.563			
SC_1			0.958		
SC_2			0.805		
SC_3			0.708		
SC_4			0.642		
SC_5			0.712		
SC_6			0.632		
CONS_1				0.836	
CONS_2				0.813	
CONS_3				0.847	
CONS_4				0.823	
CONS_5				0.861	
CONS_6				0.763	
EFFE_1					0.742
EFFE_2					0.733
EFFE_3					0.747
EFFE_4					0.822
EFFE_5					0.722
EFFE_6					0.816
INNO_1					0.747
INNO_2					0.774
INNO_3					0.807

INNO_4	0.722		
INNO_5	0.671		
INNO_6	0.856		
COOP_1		0.736	
COOP_2		0.762	
COOP_3		0.835	
COOP_4		0.752	
COOP_5		0.787	
COOP_6		0.737	
COOP_7		0.812	
COOP_8		0.850	
INT_1			0.873
INT_2			0.837
INT_3			0.807

Table 4. 2: Outer Loadings

According to the findings presented in Table 4.2, the outer loadings for all ten constructs, with the exception of ISC_6, exhibited values higher than 0.60. These values surpass the threshold of acceptability set at 0.50, as established by Chin (1998).

4.3.2. Internal consistency reliability

Internal consistency (IC) and construct reliability were assessed using the PLS-SEM generated Composite Reliability (CR) measure and Cronbach's alpha respectively. Internal consistency assumes that each block in the measurement is homogeneous. It assumes that scores for all variables have the same range and meaning (Hair Jr et al., 2017). In other words, various items measuring different constructs deliver consistent scores. Because reliability is separate for each construct, the internal consistency tests measure the reliability for each construct independently. A threshold of 1.00 for Cronbach‘s alpha, or composite reliability denotes perfect internal consistency reliability, which is unlikely to occur (Chin, 1998; J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M., 2017). The present study assessed the internal consistency reliability

by employing the CR measure, which was required to exceed a threshold of 0.70 in the PLS path models, as suggested by Henseler et al. (2009).

Cronbach's alpha is one of the most widely used metrics for reliability evaluation (Taber, 2018). According to (Taber, 2018), Cronbach's alpha reliabilities can be evaluated based on specific thresholds. A value below 0.6 would be classified as poor, while a value within the range of 0.7 is deemed acceptable. Reliability values exceeding 0.8 are considered good. According to (Taber, 2018), a minimum value of 0.7 is considered necessary to determine whether an item is capable of generating reliable measures. In the present study, the reliability of measures was evaluated by computing both Cronbach's alpha (α) and composite reliability, following the guidelines outlined by J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017), utilizing the Smart-PLS software. Table 4.5 illustrates the evaluation of construct reliability through the examination of both Cronbach's alpha (α) and CR. The results displayed in Table 4.3 indicate that all CR values, ranging from 0.870 to 0.928, surpass the specified threshold values (> 0.70). Furthermore, the Cronbach's Alpha values in the range exceeding 0.7, as shown in the table, exceed the recommended levels of acceptance, aligning with (Taber, 2018) and Sekaran's (2006) criteria.

Latent variables	**CR >0.70**	**α >0.70**
Moral Beliefs	0.913	0.913
Perceived benefit	0.888	0.893
Formal sanctions	0.881	0.887
Informal sanctions	0.865	0.870
Shame	0.884	0.889
Consistency	0.927	0.927
Effectiveness	0.894	0.895
Innovativeness	0.894	0.897
Cooperativeness	0.928	0.928
Intention	0.877	0.877

Table 4. 3: Assessment results of composite reliability and Cronbach's Alpha (α)

4.3.3. Convergent Validity

As defined by J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017), pertains to "the degree to which a measure positively correlates with other measures (indicators) of the same construct." Essentially, it assesses the extent to which variables within the same construct, measuring the same phenomenon, exhibit positive correlations with one another (D. Straub et al., 2004) or converge when compared to variables measuring different constructs. In PLS analysis, convergent validity can be established through Average Variance Extracted (AVE), as proposed by Chin (1998). AVE serves as an indicator of the extent to which a construct can account for the average variance among its indicators. It offers a comprehensive measure of convergence (Hair et al., 2013). Generally, a rule of thumb dictates that AVE should exceed 0.5, implying that the construct can explain at least 50% of the variance and indicating satisfactory convergence (Hair et al., 2013).

4.3.3.1 The Average Variance Extracted

AVE measure quantifies the degree to which a construct can account for the variability observed in its indicators, expressed as a percentage. The statement refers to a summary indicator of convergence as discussed by Hair et al. (2013). According to Chin (1998) and Hair et al. (2013), it is generally accepted that the average variance extracted should exceed 0.5. This threshold indicates that the construct under consideration explains at least 50% of the variance and suggests satisfactory convergence. According to the findings presented in Table 4.4, the analysis reveals that the average variance extracted values fall within the range of 0.524 to 0.778, surpassing the established threshold value of 0.50. Therefore, the confirmation of the convergent validity of constructs has been established.

Latent variables	AVE >**0.50**
Moral Beliefs	0.778
Perceived benefit	0.573
Formal sanctions	0.558
Informal sanctions	0.524
Shame	0.565
Consistency	0.679
Effectiveness	0.585
Innovativeness	0.585
Cooperativeness	0.616
Intention	0.705

Table 4. 4: Assessment results of average variance extracted

4.3.4. Discriminant validity

As described by J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017) discriminant validity measures the extent to which a latent variable is genuinely distinct from other latent variables. Put differently, it evaluates whether the measurement items comprising a specific construct are indeed different from those items intended to represent other constructs (D. Straub et al., 2004). In assessing discriminant validity within PLS-SEM path models, two widely recognized criteria are employed: cross-loadings and the Fornel-Larcker criterion, also known as the square root of the average variance extracted. Additionally, we employed the Heterotrait-Monotrait Ratio of Correlations (HTMT) of correlations, a novel approach for evaluating discriminant validity.

4.3.4.1 The square root of the average variance extracted

For each factor, as well as the correlation coefficients between these factors and other factors, are displayed in Table 4.5. According to the findings presented in Table 4.5, none of the correlations observed were equal to or exceeded the square root of the average variance

extracted. This suggests that there is evidence of discriminant validity. Specifically, the diagonal elements, which represent the square root of AVE, were found to be greater than the off-diagonal elements in the respective rows and columns, indicating that the discriminants are valid. Similarly, Gefen and Straub (2005) argue that there is a lack of established guidelines regarding the magnitude by which the average variance extracted should be larger. According to the Fornel-Larcker criteria, the criterion of discriminant validity for the measurements of the model has been met.

Latent variables	1	2	3	4	5	6	7	8	9	10
Shame	**0.751**									
Consistency	0.256	**0.824**								
Cooperativeness	-0.031	0.440	**0.785**							
Effectiveness	0.025	0.514	0.382	**0.765**						
Formal sanctions	0.732	0.147	-0.112	-0.003	**0.747**					
Informal sanctions	0.624	0.187	-0.033	0.055	0.721	**0.724**				
Innovativeness	0.001	0.256	0.344	0.224	-0.005	0.119	**0.765**			
Moral Beliefs	0.459	0.071	-0.147	0.009	0.466	0.414	-0.014	**0.882**		
Perceived benefit	0.672	0.120	-0.126	0.019	0.741	0.617	0.021	0.454	**0.757**	
Intention	0.570	0.535	0.312	0.395	0.562	0.554	0.370	0.339	0.551	**0.839**

Table 4. 5: Discriminant validity assessment (Fornel–Larcker criteria)

Notes: The numbers in the diagonal are the square root of AVE.

4.3.4.2 Cross-loadings

Cross-loadings refer to the situation where indicators exhibit a higher loading on their corresponding construct compared to any other reflective construct (Hanafiah, 2020). This occurrence serves as evidence that the construct in question is distinct and captures a certain

phenomenon that is not accounted for by other measurement items (Joseph F Hair Jr et al., 2021; J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M., 2017). Therefore, this finding suggests that there is sufficient evidence of discriminant validity. According to Gefen and Straub (2005), there is currently a lack of established thresholds for factor loadings in order to determine discriminant validity in PLS path models.

According to Chin (1998) and Gefen and Straub (2005), if all indicators in the correlation score matrix exhibit higher loadings on their respective latent variables compared to any other constructs, and if each latent variable demonstrates the highest loadings with its own items, this can be considered evidence supporting discriminant validity. According to the findings presented in Table 4.6, the analysis of the indicators' cross loading demonstrated that none of the indicators exhibited a higher loading on a construct that is in opposition to it (J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M., 2017). Therefore, this provides confirmation that there is sufficient discriminant validity among all of the constructs.

	Shame	**Consistency**	**Cooperativeness**	**Effectiveness**	**Formal sanctions**	**Informal sanctions**	**Innovativeness**	**Moral Beliefs**	**Perceived benefit**	**Intention**
MB_1	0.403	0.036	-0.159	-0.015	0.416	0.366	-0.014	**0.902**	0.437	0.293
MB_2	0.411	0.073	-0.103	0.009	0.395	0.370	0.000	**0.869**	0.378	0.312
MB_3	0.402	0.081	-0.126	0.029	0.423	0.360	-0.024	**0.876**	0.386	0.292
PBC_1	0.644	0.143	-0.132	-0.007	0.680	0.595	0.006	0.418	**0.946**	0.530
PBC_2	0.550	0.109	-0.033	0.036	0.614	0.510	0.033	0.418	**0.838**	0.477
PBC_3	0.468	0.085	-0.082	0.007	0.538	0.410	0.015	0.314	**0.695**	0.375
PBC_4	0.441	0.112	-0.115	0.059	0.504	0.390	0.023	0.304	**0.668**	0.374
PBC_5	0.476	0.040	-0.110	-0.005	0.505	0.418	0.011	0.302	**0.675**	0.345
PBC_6	0.446	0.040	-0.109	-0.001	0.504	0.450	0.008	0.282	**0.677**	0.371
SC_1	**0.958**	0.235	-0.058	-0.014	0.674	0.623	0.002	0.434	0.647	0.561

SC_2	**0.805**	0.169	-0.011	0.013	0.595	0.526	-0.007	0.378	0.567	0.405
SC_3	**0.708**	0.199	0.014	0.045	0.527	0.441	0.060	0.316	0.464	0.407
SC_4	**0.642**	0.155	-0.054	-0.012	0.479	0.401	-0.046	0.309	0.428	0.349
SC_5	**0.712**	0.217	0.031	0.064	0.516	0.425	-0.002	0.337	0.448	0.448
SC_6	**0.632**	0.177	-0.059	0.029	0.482	0.350	-0.004	0.273	0.439	0.371
CONS_1	0.226	**0.836**	0.374	0.451	0.098	0.152	0.152	0.060	0.101	0.454
CONS_2	0.231	**0.813**	0.343	0.405	0.143	0.145	0.256	0.073	0.113	0.415
CONS_3	0.232	**0.847**	0.367	0.436	0.136	0.159	0.173	0.094	0.097	0.463
CONS_4	0.206	**0.823**	0.360	0.398	0.129	0.151	0.261	0.037	0.102	0.445
CONS_5	0.197	**0.861**	0.407	0.456	0.123	0.164	0.205	0.043	0.087	0.448
CONS_6	0.172	**0.763**	0.319	0.392	0.096	0.155	0.223	0.046	0.095	0.421
COOP_1	-0.012	0.293	**0.736**	0.241	-0.089	-0.066	0.296	-0.154	-0.104	0.244
COOP_2	-0.014	0.327	**0.762**	0.298	-0.066	-0.049	0.270	-0.098	-0.089	0.246
COOP_3	-0.047	0.361	**0.835**	0.323	-0.140	-0.049	0.280	-0.144	-0.121	0.234
COOP_4	0.011	0.361	**0.752**	0.305	-0.051	-0.026	0.225	-0.072	-0.096	0.239
COOP_5	-0.052	0.360	**0.787**	0.293	-0.112	-0.041	0.277	-0.116	-0.116	0.208
COOP_6	-0.054	0.315	**0.737**	0.261	-0.119	-0.025	0.251	-0.120	-0.133	0.234
COOP_7	-0.041	0.354	**0.812**	0.307	-0.073	0.007	0.279	-0.141	-0.097	0.261
COOP_8	0.014	0.384	**0.850**	0.359	-0.056	0.032	0.284	-0.079	-0.044	0.290
EFFE_1	0.001	0.387	0.285	**0.742**	0.033	0.024	0.143	-0.015	0.012	0.301
EFFE_2	0.032	0.342	0.283	**0.733**	0.030	0.090	0.153	0.044	0.075	0.329
EFFE_3	0.045	0.405	0.266	**0.747**	-0.003	0.035	0.141	0.032	0.004	0.299
EFFE_4	0.032	0.440	0.305	**0.822**	-0.016	0.037	0.195	0.011	0.017	0.304
EFFE_5	-0.042	0.377	0.286	**0.722**	-0.059	0.006	0.199	-0.016	-0.051	0.256
EFFE_6	0.042	0.403	0.324	**0.816**	0.000	0.060	0.195	-0.014	0.027	0.321
FSC_1	0.673	0.164	-0.080	-0.005	**0.947**	0.679	-0.036	0.452	0.692	0.567
FSC_2	0.524	0.119	-0.087	-0.014	**0.734**	0.525	0.059	0.338	0.551	0.426
FSC_3	0.550	0.149	-0.100	0.020	**0.733**	0.515	0.004	0.313	0.537	0.431
FSC_4	0.478	0.042	-0.084	-0.008	**0.644**	0.478	-0.029	0.329	0.476	0.325
FSC_5	0.499	0.084	-0.089	-0.011	**0.669**	0.486	-0.021	0.297	0.519	0.340
FSC_6	0.534	0.078	-0.069	0.001	**0.715**	0.522	0.007	0.341	0.522	0.391
INNO_1	0.036	0.179	0.231	0.172	0.044	0.123	**0.747**	-0.018	0.049	0.296

INNO_2	0.018	0.190	0.239	0.151	0.059	0.149	**0.774**	0.006	0.063	0.314
INNO_3	0.025	0.199	0.267	0.171	0.037	0.136	**0.807**	0.047	0.041	0.309
INNO_4	-0.048	0.185	0.262	0.182	-0.044	0.054	**0.722**	-0.037	-0.024	0.253
INNO_5	-0.021	0.169	0.257	0.134	-0.044	0.023	**0.671**	-0.028	-0.019	0.253
INNO_6	-0.008	0.247	0.321	0.212	-0.074	0.056	**0.856**	-0.040	-0.017	0.273
ISC_1	0.580	0.192	-0.025	0.079	0.699	**0.952**	0.140	0.380	0.571	0.543
ISC_2	0.430	0.200	0.023	0.086	0.501	**0.712**	0.125	0.259	0.424	0.436
ISC_3	0.465	0.152	-0.054	0.047	0.509	**0.745**	0.036	0.330	0.479	0.415
ISC_4	0.414	0.119	0.029	-0.004	0.447	**0.627**	0.071	0.267	0.386	0.329
ISC_5	0.429	0.058	-0.062	-0.009	0.506	**0.684**	0.099	0.316	0.439	0.338
ISC_6	0.364	0.064	-0.058	0.020	0.427	**0.563**	0.024	0.226	0.348	0.299
INT_1	0.504	0.439	0.247	0.325	0.510	0.500	0.301	0.307	0.501	**0.873**
INT_2	0.466	0.449	0.268	0.351	0.473	0.455	0.328	0.255	0.464	**0.837**
INT_3	0.464	0.461	0.271	0.318	0.430	0.438	0.304	0.291	0.420	**0.807**

Table 4. 6: Cross loadings for individual measurement items

4.3.4.3 Heterotrait-Monotrait Ratio of Correlations

The HTMT is a relatively new method for assessing discriminant validity in SEM studies (Henseler et al., 2015). It helps ensure that constructs are distinct from each other by comparing the correlations between constructs and the average correlations within constructs. A threshold value of less than 0.90 is commonly used to confirm that discriminant validity has been achieved, meaning that constructs are adequately differentiated from one another (Henseler et al., 2015).

In this study, the HTMT was employed to strengthen the assessment of discriminant validity, following the recommendation by Henseler et al. (2015). As indicated in Table 4.7, the HTMT ratios of correlations for each construct are all below 0.9, which signifies that discriminant validity has been satisfactorily established. The HTMT ratios for all constructs met this criterion, providing further evidence of discriminant validity.

Latent variables	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

1.	Shame									
2.	Consistency	0.254								
3.	Cooperativeness	0.059	0.438							
4.	Effectiveness	0.051	0.513	0.379						
5.	Formal sanctions	0.712	0.141	0.113	0.042					
6.	Informal sanctions	0.602	0.181	0.066	0.071	0.699				
7.	Innovativeness	0.057	0.254	0.342	0.221	0.069	0.119			
8.	Moral Beliefs	0.451	0.072	0.147	0.034	0.458	0.409	0.038		
9.	Perceived benefit	0.649	0.116	0.132	0.052	0.720	0.597	0.049	0.445	
10.	Intention	0.560	0.536	0.312	0.395	0.549	0.541	0.369	0.339	0.539

Table 4. 7: Discriminant validity assessment using the HTMT criterion

In conclusion, the reliability and validity of the measurement model are demonstrated by the fact that it satisfies a variety of reliability and validity criteria. Therefore, the latent variables that were developed by using this measurement model possess sufficient validity and reliability for the purpose of putting the conceptual model and the associated hypotheses that were proposed earlier to the test. The discussion of the structural model will continue in the subsequent section.

4.4 Assessment of the Structural Model

After establishing a measurement model of satisfactory quality, as suggested by Joseph F Hair Jr et al. (2021), the study advances to the subsequent phase, which involves the evaluation of the structural model. This assessment of the structural model encompasses several critical steps to ensure its robustness and reliability. The procedure for evaluating the structural model includes the following key components:

Assessment of Multicollinearity: One of the initial steps is to examine the presence of multicollinearity within the model. Multicollinearity refers to the situation where predictor variables in a regression model are highly correlated, which can lead to unstable and unreliable estimates of coefficients. Coefficient of Determination (R^2): R^2 is a crucial statistical metric used to measure the proportion of variance in the dependent variable that can be explained by the independent variables in the model. It provides insights into the goodness fit of the structural model. Q2: Predictive Relevance: Q2 is a measure of predictive relevance and assesses the model's ability to predict the endogenous constructs accurately. It helps determine whether the structural model can effectively explain and predict the observed data. F2 Effect Size: The f2 effect size is employed to gauge the practical significance of relationships within the structural model. It indicates the strength of the associations between variables, allowing researchers to assess the practical importance of their findings. Estimation of Path Coefficients: The estimation of path coefficients involves calculating the relationships between the latent constructs in the structural model. Path coefficients elucidate the strength and direction of the connections between variables, providing insights into the hypothesized relationships.

This comprehensive evaluation of the structural model, following the guidance of Ghasemy et al. (2020), Hair et al. (2021), and Sarstedt et al. (2017), ensures that the research study not only establishes a robust measurement model but also effectively examines the relationships and predictions inherent in the structural framework. Table 4.8 also summarizes the criteria for the four key assessments of structural model, adopted from (Ghasemy et al., 2020; Hair et al., 2021; Sarstedt et al., 2019). In this study, Hair et al. (2021) procedure of assessment will be employed since it is more comprehensive and up to date.

Test	Method	Rule of Thumb	Source
Model validity	R2 - Coefficient of determination	Values of approximately 0.670 are considered to be substantial, values around .333 moderate, and values around 0.190 weak.	(Ghasemy et al., 2020)
Model validity	Path coefficients	For sample sizes of up to 1000, path coefficients above 2.0 are significant, and values below 0.10 are not.	(Hair et al., 2021)
Model Validity	f2 - effect size	Values of .020, .150, and .350 indicate the predictor variable's low, medium, or large effect in the structural model.	(Ghasemy et al., 2020; Hair et al., 2021; Sarstedt et al., 2019)
Model validity	Q2 – predictive relevance	The proposed threshold value is Q2 > 0.	(Ghasemy et al., 2020; Hair et al., 2021; Sarstedt et al., 2019)

Table 4. 8: Criteria used for the assessment of structural model

4.4.1 Collinearity Assessment in the Structural Model

In this particular section, the assessment of collinearity for multi-dimensional constructs necessitates the individual examination of each set of predictor constructs with respect to every component of the structural model. According to the recommendation put forth by J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017), it is suggested that the values of Variance Inflation Factor (VIF) should ideally be below 5.0. In this study, a total of nine components of the model were identified and subsequently subjected to collinearity assessment. According to the data presented in Table 4.9, it can be observed that all exogenous constructs exhibit VIF values below 5.0. The VIF values range from 1.306 to 3.622, indicating the absence of any multicollinearity concerns within the structural model. The findings indicate that all of the values

obtained from the VIF analysis are lower than the recommended threshold of 5.00, as proposed by J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017). Hence, the elimination of constructs was unnecessary.

Latent variables	Information security policy compliance intention
Moral Beliefs	1.423
Perceived benefit	2.689
Formal sanctions	3.622
Informal sanctions	2.518
Shame	2.866
Consistency	1.918
Effectiveness	1.53
Innovativeness	1.306
Cooperativeness	1.574

Table 4. 9: VIF values of structural model variables

4.4.2 Coefficient of determination (R^2)

An indispensable factor in evaluating the PLS structural equation model is the coefficient of determination (R^2) for each latent variable. The term "R^2" denotes the fraction of the overall variability observed in the dependent variable that can be accounted for by the variability in the independent or predictor variable (Chin, 1998). The measurement assesses the associations between latent variables and offers an estimate of the proportion of variance in the latent variable that is accounted for by its total variance. In order to demonstrate a minimum level of explanatory power, it is necessary for the R^2 of an endogenous latent variable to surpass a sufficient threshold. Based on the criteria established by Jacob Cohen (2013), R^2 values of 0.02, 0.13, and 0.26 are indicative of weak, moderate, and substantial levels of explanatory power, respectively. The findings of this study, as presented in Table 4.10, indicate that the coefficient of determination (R^2) for information security policy compliance intention is 0.813. This value suggests that approximately 81.3% of the variability in information security policy compliance intention can

be explained by the independent variables. Thus, for information security policy compliance intention, the R^2 value is considered substantial.

Endogenous constructs	R^2
Information security policy compliance intention	0.813

Table 4. 10: Coefficient of determination (R^2 value)

4.4.3 Predictive capacity or Predictive relevance (Q^2)

Predictive relevance refers to the evaluation of a model's ability to accurately predict the indicators of an endogenous latent variable (Latan et al., 2017). As stated by Latan et al. (2017), the Q^2 metric serves as an indicator of the model's ability to accurately reconstruct observed values and estimate its parameters. Therefore, the test holds significance in PLS path modelling and can serve as a valuable tool for evaluating structural models. The Stone-Geisser test, was developed by Stone and Geisser (Chin, 2008). It is widely recognized as a prominent method for assessing the predictive validity of a model. Models that have a Q^2 value greater than zero, when applied to reflective endogenous latent constructs, demonstrate the predictive relevance of the path model for the specific construct in question. Such models are regarded as possessing predictive relevance.

The Q^2 statistics are generated through a procedure that systematically excludes one case at a time, guided by a predetermined omission distance. The algorithm employs a technique known as "blindfolding" in PLS-SEM to omit every xth data point, where x represents the omission distance. This process involves re-estimating the structural model using the remaining cases after omission and predicting the values of the blindfolded cases based on the remaining parameters.

The blindfolding procedures are exclusively implemented on the reflective endogenous latent variables, as stated by Henseler et al. (2015). This methodology offers two types of predictive relevance (Q^2): cross-validated communality and cross-validated redundancy, which can be obtained through the implementation of blindfolding procedures (Tenenhaus et al., 2005). According to J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017), it is suggested that

the cross-validated redundancy be utilized as a metric for evaluating Q^2. This is because it incorporates the essential component of the path model, namely the structural model, in order to predict the excluded data points (J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M., 2017). The anticipated outcome of Q^2 is to demonstrate the predictive ability of the path model in relation to the initially observed values.

The aforementioned procedure was executed individually for each of the endogenous variables in the model. The omission distance was set at a threshold of 8, as suggested by Wold (1982 in (Tenenhaus, 2005 #652@@author-year) and J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017). The findings presented in Table 4.11 depict the blindfolding outcomes of the cross-validated redundancy (Q^2) for the latent endogenous variable in the direct relationships model employed in this research. The presence of cross-validated redundancy (Q2) in the context of Information security policy compliance intention (0.530) is greater than zero, suggests that the model has predictive value for this factor (Latan et al., 2017) (Chin, 1998; Latan & Noonan, 2017).

Endogenous constructs	Q^2
Information security policy compliance intention	0.530

Table 4. 11: Results of cross-validated redundancy (Q^2)

4.4.4 Effect Size (f^2)

The test of effect size is considered a fundamental component in PLS-SEM path modelling, as discussed by Chin (1998) and Henseler et al. (2009). In a statistical context, in addition to assessing path coefficients, effect size serves as an alternative measure for quantifying the magnitude of the association between the independent variable and the dependent variable (Hair et al., 2021; J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M., 2017). The power of variance explained is directly influenced by the magnitude of effect size. Consequently, path coefficients may exhibit significance without necessarily indicating the strength of the relationship. The effect size test is used to estimate the extent to which the latent construct, which is connected to the path, increases the R^2 values of the associated endogenous construct. This increase is

measured relative to the proportion of unexplained variance of the endogenous construct that can be attributed to the latent construct (Chin, 1998). The measurement of this is typically conducted using the Cohen's pseudo-f or f^2 test (Chin, 1998; J Cohen, 1998), with f^2 being defined as:

$f^2 = (R^2$ full model - R^2 partial model) / (1- R^2 full model).

The term "full model" refers to the original model that includes all of the model constructs. On the other hand, the term "partial model" refers to an alternative model that is created by removing a specific construct from the original model. Hence, the alteration in the R^2 coefficient when a particular construct is omitted from the model indicates the extent to which the excluded construct significantly influences the endogenous construct to which the removed latent variable is directly connected. The magnitude of the independent construct's influence increases as the value of f^2 increases. Values of 0.02, 0.15, and 0.35 can be categorized as representing small, medium, and large effects, respectively (Chin, 1998; J Cohen, 1998; J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M., 2017).

In order to assess the magnitude of the effect in this particular model, the measure of f^2 was utilized for each endogenous construct. The outcomes of the f^2 test are presented in Table 4.12 as depicted below. The findings indicate that each of the latent constructs exhibit a limited impact on the original model, demonstrating a weak contribution. In brief, the findings presented in Table 4.12 indicate that the influence of moral belief (Hypothesis1), perceived benefit (Hypothesis2), formal sanction (Hypothesis3), informal sanction (Hypothesis4), and shame (Hypothesis5) on employees' intention towards ISP compliance is have weak effects on their respective endogenous constructs.

Path	Hypothesis	f2
Moral Beliefs -> Information security policy compliance intention	1	0.041
Perceived benefit -> Information security policy compliance intention	2	0.059
Formal sanctions -> Information security policy compliance intention	3	0.080
Informal sanctions -> Information security policy compliance intention	4	0.042
Shame -> Information security policy compliance intention	5	0.076

Table 4. 12: f^2 effect size of structural model variables

4.4.5 Assessment of the Structural Model Path Coefficients

According to Henseler et al. (2009), a frequently employed approach to evaluate the structural model involves examining the algebraic sign, magnitude, and significance of the path coefficients connecting latent variables. Any paths that exhibit algebraic signs contrary to the theoretical expectation are not supportive of the assumed hypotheses. The structural path coefficients offer a limited empirical confirmation of the theoretically hypothesized connections between the constructs in the model (Henseler et al., 2009). This will enable us to evaluate the validity of the hypothesized relationships pertaining to ISP compliance.The second assumption in evaluating path coefficients is that each individual path should possess a certain level of magnitude to effectively demonstrate the significance of the relationship between the endogenous and exogenous constructs (Chin, 1998; J. F. Hair Jr, Hult, G. T. M., Ringle, C., & Sarstedt, M., 2017). The determination of the statistical significance of paths can be achieved by employing re-sampling techniques that produce t-values.

According to Chin (1998) and Hair et al. (2017), in order to achieve a significance level of .050, it is generally required to have beta values greater than 0.20 and t-values equal to or exceeding 1.96. The parameters were derived by extracting t-statistics values from the path coefficient table generated by Smart-PLS. In the assessment of the structural model, the statistical significance of path coefficients was examined using a bootstrapping resampling procedure with 5000 subsamples (Streukens and Leroi-Werelds, 2016).

The default settings, including parallel processing and no sign changes were employed for this analysis. According to the findings presented in Table 4.13, all but two of the paths examined in the study were found to be statistically significant. Among the coefficient values provided in the results, the coefficient value with the highest magnitude is 0.209, which corresponds to the path "Formal sanctions -> Intention." This path exhibited the highest relationship strength between the variables. Conversely, the coefficient value with the lowest magnitude is 0.014, which

corresponds to the path "Informal sanctions x Consistency -> Intention." This path exhibited the weakest relationship strength among the variables.

Hyp_No	Path	Beta value	T-Statistics	P-Values	Results
H1	Moral Beliefs -> Intention	0.091	2.977	0.003	Accept
H2	Perceived benefit -> Intention	0.162	4.296	0.001	Accept
H3	Formal sanctions -> Intention	0.209	4.826	0.001	Accept
H4	Informal sanctions -> Intention	0.129	3.837	0.001	Accept
H5	Shame -> Intention	0.200	4.223	0.001	Accept
H6	Moral Beliefs x Consistency -> Intention	0.086	2.446	0.014	Accept
H7	Perceived benefit x Effectiveness -> Intention	0.086	3.359	0.001	Accept
H8	Formal sanctions x Consistency -> Intention	0.151	4.454	0.001	Accept
H9	Informal sanctions x Consistency -> Intention	-0.014	0.510	0.610	Reject
H10	Perceived benefit x Innovativeness -> Intention	0.044	1.646	0.100	Reject
H11	Shame x Cooperativeness -> Intention	0.112	4.535	0.001	Accept
	Consistency -> Intention*	0.214	6.593	0.001	Significant
	Effectiveness -> Intention*	0.112	3.846	0.001	Significant
	Innovativeness -> Intention*	0.115	3.936	0.001	Significant
	Cooperativeness -> Intention*	0.096	3.312	0.001	Significant

Table 4. 13 T-statistics values for path coefficients between constructs

*Not hypothesized paths

4.5 Chapter summary

The primary objective of this chapter was to subject the instrument to a series of rigorous scientific processes, aimed at evaluating and validating its efficacy within the context of existing research. This validation procedure encompasses both the measurement and structural aspects of the model. Accordingly, the chapter meticulously adhered to established criteria for evaluating the measurement model, which included assessments of internal consistency reliability, indicator reliability, convergent validity, and discriminant validity. Additionally, in line with the criteria for assessing the structural model, considerations such as construct multi-collinearity, coefficient of determination, path coefficients, effect size, and predictive relevance were thoroughly scrutinized.

Upon thorough examination, it was determined that all paths investigated in the study exhibited statistical significance, with the exception of Hypotheses H9 and H10. Specifically, Hypothesis H9, positing a relationship between "Informal sanctions" and "Intention," was found to lack statistical significance (p-value = 0.610) and was consequently rejected. Similarly, Hypothesis H10, proposing a linkage between "Perceived benefit" and "Intention," also failed to attain statistical significance (p-value = 0.100) and was thus dismissed. Consequently, it can be inferred that the model, comprising a psychometrically robust set of constructs, has now reached a stage where its findings can be interpreted with confidence.

Moving forward, the subsequent chapter will delve into the interpretation and implications of the results gleaned from this rigorous validation process, offering deeper insights into the implications of the findings and their broader significance within the research domain.

CHAPTER FIVE: FINDING AND DISCUSSION

5.1 Introduction

This chapter provides a discussion of the outcomes of each hypothesis. As stated in the introductory chapter, the primary objective of this research is to investigate the moderating effect of organizational culture on the relationship between perceived benefits, moral beliefs, formal sanctions, informal sanctions, and shame, and employees' intention to comply with information security policy. Through the utilization of a dataset obtained from various organizations in Ethiopia, our study reveals compelling evidence regarding the significant impact of organizational culture dimensions on the efficacy of information security policy countermeasures. This influence is observed in both strengthening and weakening the relationship between information security policy countermeasures and other crucial variables, as demonstrated by the RCT. Furthermore, our findings shed light on the connection between organizational culture dimensions and employees' intention to comply with ISP. Therefore, the subsequent paragraphs will outline the principal discoveries of the investigation.

5.2 Findings and discussions on the structural model

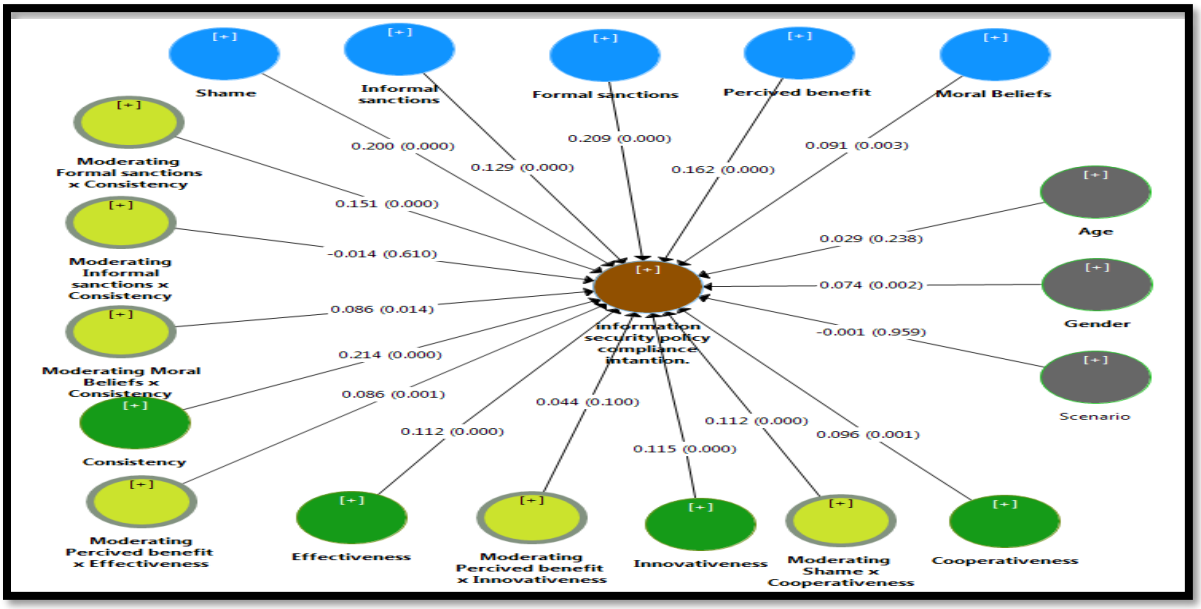


Figure 5. 1: The Structural Model

Hypotheses	Results
H1: Moral belief is positively related to employees' intention towards ISP compliance.	Supported
H2: Perceived benefit of compliance is positively related to employees' intention towards ISP compliance.	Supported
H3: Formal sanction is positively related to employees' intention towards ISP compliance.	Supported
H4: Informal sanction is positively related to employees' intention towards ISP compliance.	Supported
H5: Shame is positively related to employees' intention towards ISP compliance.	Supported
H6: Consistency culture strengthens the positive effect between moral beliefs and compliance intention.	Supported
H7: Effectiveness culture strengthens the positive effect between perceived benefits and compliance intention.	Supported
H8: Consistency culture strengthens the positive effect between formal sanctions and compliance intention.	Supported
H9: Consistency culture strengthens the positive effect between informal sanctions and compliance intention.	Rejected
H10: Innovativeness culture strengthens the positive effect between Perceived benefits and compliance intention.	Rejected
H11: Cooperativeness culture strengthens the positive effect between shame and compliance intention.	Supported

Table 5. 1 Summary of Hypotheses testing

In the following section the findings related to the individual hypotheses are discussed in detail.

5.2.1 Moral belief is positively related to employees' intention towards ISP compliance.

Hypothesis H1 posits that there exists a positive relationship between employees' moral beliefs and their intention to comply with their organization's information security policy. This

relationship is examined through statistical analysis, with the hypothesis being supported by the data presented in Table 5.1. The statistical tests conducted reveal that the p-values associated with this hypothesis are less than 0.05, establishing its validity. Consequently, H1, which asserts that "moral belief is positively related to employees' intention towards ISP compliance," is accepted based on the results, which demonstrate a positive relationship between moral beliefs and intention.

The standardized estimate, further reinforcing the findings of H1, demonstrates a positive and statistically significant relationship (H1: $\beta = 0.091$; t-value= 2.977; $p < 0.01$) between moral beliefs and employees' intention to comply with ISP. In essence, this indicates that as employees' moral beliefs and commitments strengthen, so does their intent to refrain from violating their organization's ISP. This observation aligns closely with the fundamental principles of rational choice theory as proposed by Becker in 1968. It suggests that individuals, when faced with choices, are more likely to make decisions that adhere to societal norms and values when they possess strong moral convictions.

Furthermore, these findings find support in criminological studies, which have consistently reported that individuals with lower moral beliefs or weaker personal norms tend to exhibit a greater inclination toward engaging in deviant behaviors. For instance, research has shown a correlation between lower moral convictions and involvement in corporate crime (Paternoster and Simpson, 1996) or tax evasion (Wenzel, 2004). This alignment between moral beliefs and desirable behavior has also been explored in psychology, with studies indicating that robust moral reasoning contributes to the development of positive behaviors (Blasi, 1980; King and Mayhew, 2002; Rest, 1986, as cited in Myyry et al., 2009).

Moreover, it is important to note that, in the existing body of literature on information security, it has been consistently observed that personal norms and moral beliefs play a significant role in influencing employees' intentions to comply (Vance et al., 2020). The studies conducted by (D'Arcy et al., 2009; M. Siponen, 2002; M. Siponen et al., 2012) are relevant to this topic. This study highlights the significance of moral beliefs in influencing individuals' intentions to comply

with ISP regulations. It also provides additional empirical evidence that supports the acceptance of Hypothesis H1.

In conclusion, the acceptance of Hypothesis H1 is well-founded and substantiated by both statistical evidence and its alignment with established theories across disciplines. The relationship between moral beliefs and employees' intention to comply with ISPs is not only statistically significant but also conceptually consistent with findings in criminology, psychology, and the ISS literature. This acceptance highlights the crucial role of moral beliefs in shaping compliance intentions and has practical implications for enhancing information security practices within organizations.

5.2.2 Perceived benefit of compliance is positively related to employees' intention towards ISP compliance.

The acceptance of Hypothesis H2, which asserts that "perceived benefit of compliance is positively related to employees' intention towards ISP compliance," is supported by substantial evidence and aligns with well-established theories across various academic domains. This acceptance reflects the critical role that perceived benefits play in shaping employees' intentions towards compliance with information security policies.

First and foremost, the statistical analysis, as reflected Table 5.1, underscores the significance of the perceived benefit of compliance in influencing employees' intentions regarding ISP compliance. The statistical parameters, including a significant positive beta coefficient (β= 0.162), a high t-value (t-value= 4.296), and a p-value less than 0.01, all provide strong empirical support for Hypothesis H2. This suggests that as employees perceive greater benefits in complying with ISP, they are more likely to exhibit an intention to comply.

Furthermore, the acceptance of Hypothesis H2 finds theoretical support in the RCT, as mentioned in the provided text. RCT posits that individuals make choices by evaluating the outcomes and perceived benefits of each alternative and selecting the one that promises greater satisfaction or perceived benefits (McCarthy, 2002). Applied to the context of ISP compliance, employees who perceive benefits or advantages in adhering to these policies are more inclined

to express intentions to comply. This aligns with the fundamental principles of RCT and reinforces the acceptance of Hypothesis H2.

This finding aligns with previous research conducted in the field of criminology (Ducan et al., 2005; Wood et al., 1997). This discovery indicates that when employees perceive benefit of adhering to information security policies, they are more inclined to comply with them. Additionally, empirical studies within the information security literature provide further validation for the relationship between perceived benefits and compliance intentions. Vance and Siponen (2012) found that employees who perceived benefits in complying with information security policies were more likely to express positive intentions. This study's findings support Hypothesis H2, which posits a positive relationship between perceived benefit of compliance and employees' intention towards ISP compliance.

This suggests that when employees perceive advantages in adhering to ISP guidelines, they are more inclined to exhibit an intention to comply. In contrast, Li et al. (2010) reported a significant negative influence of perceived benefits on employees' compliance intention with the internet use policy. This finding highlights the complexity of the relationship between perceived benefits and compliance intentions, as it suggests a different direction of influence. However, it's essential to note that Hypothesis H2 specifically focuses on ISP compliance and proposes a positive relationship between perceived benefit of compliance and employees' intention towards ISP compliance, which may differ from the dynamics observed in the context of internet use policy compliance.

To sum up, the validation of Hypothesis H2 is supported by substantial statistical evidence and is consistent with established theories such as RCT. Furthermore, this assertion is supported by empirical research in the fields of information security and criminology, which consistently demonstrates that employees' perceptions of the advantages of adhering to compliance regulations significantly influence their intentions regarding compliance with information security policies.

5.2.3 Formal sanction is positively related to employees' intention towards ISP compliance.

The acceptance of Hypothesis H3, which posits a positive relationship between "formal sanction" and employees' intention towards ISP compliance, is substantiated by a robust theoretical foundation and strong empirical evidence. Hypothesis H3 proposes a positive relationship between formal sanctions and employees' intention towards ISP compliance, and statistical analysis in Table 5.1 firmly supports this hypothesis, with a p-value less than 0.01, signifying statistical significance. The findings (H3: $\beta = 0.209$; t-value= 4.826; $p < 0.01$) elucidate a positive and substantial association between formal sanctions and employees' intention to comply with ISP.

This acceptance underscores the pivotal role of formal sanctions as an effective deterrence mechanism in shaping employees' intentions to comply with ISP. Formal sanctions, explicit penalties imposed for specific forms of misconduct, are important to deterrence theory, an extension of RCT. Rational choice theory posits that the imposition of formal sanctions can effectively deter undesirable behaviors. This theoretical premise finds empirical support, as demonstrated by Straub Jr and Nance (1990) research on computer abuse, where formal sanctions effectively deterred users from engaging in such misconduct. Similarly, D'Arcy et al. (2009) established that the formal sanctions significantly influenced users' intentions regarding computer abuses.

Moreover, in their study, Hu et al. (2010) discovered a significant relationship between the implementation of formal sanctions and the impact it had on employees' intentions to engage in computer offences. Also, the findings of our study align with previous research conducted in the field of criminology, as evidenced by the works of Raymond Paternoster and Simpson (1996) and Pratt et al. (2006).

Besides, the results of the first hypothesis shed light on the multifaceted role of formal sanctions in the context of ISP compliance. It was revealed that formal sanctions had influence on employees' intention, implying that organizations employing deterrence mechanisms, including formal rules and policies assisted by sanctions, are more likely to reduce employees' intentions

of noncompliance with their organizations ISP. While some inconsistencies exist in the literature regarding the impact of formal sanctions on reducing computer abuse or information security misuse, the results of this study align with research findings in the domains of criminology and information security.

In conclusion, the acceptance of Hypothesis H3 is firmly grounded in theoretical principles and fortified by compelling empirical evidence. This recognition underscores the crucial role formal sanctions play in shaping employees' intentions to comply with the ISP and their potential to effectively deter non-compliance. These findings not only align with established theories but also contribute to a deeper understanding of the relationship between formal sanctions and ISP compliance across different organizational contexts, including those in developing economies.

5.2.4 Informal sanction is positively related to employees' intention towards ISP compliance.

Hypothesis H4 posits a positive relationship between the adoption of informal sanctions and employees' intentions towards ISP compliance. This hypothesis is substantiated through statistical analysis, with a focus on the coefficient of the path "adoption of informal sanctions -> Intention." The statistical tests conducted provide robust support for H4, as evidenced in Table 5.1 the p-value being less than 0.001. Consequently, the hypothesis that "informal sanction is positively related to employees' intention towards ISP compliance" is unequivocally accepted.

The standardized estimate further strengthens the case for H4 by demonstrating a positive and statistically significant relationship (H4: $\beta = 0.129$; t-value = 3.837; $p < 0.01$) between informal sanctions and employees' intention to comply with ISP. This finding underscores the notion that the adoption of informal sanctions is associated with a heightened intention among employees to adhere to ISP requirements. Such a positive correlation between informal sanctions and compliance intention has significant implications for organizations aiming to bolster their information security practices.

The landscape of previous research into ISP compliance behavior reveals a degree of variability and mixed results. Several studies, including those by Johnston et al. (2015), Ifinedo (2014) and

Chen et al. (2018), have explored this domain, yielding diverse outcomes. Some of these studies have suggested that the efficacy of informal sanctions in promoting ISP compliance is not consistently reliable, as indicated by Ifinedo (2016).

In contrast, Johnston et al. (2015) reported that informal sanctions did not exhibit a direct impact on ISP compliance. These findings have contributed to a nuanced understanding of the role of informal sanctions in the context of ISP compliance. However, it is crucial to note that the research landscape is not uniform in its conclusions. Certain studies, such as those by Silic et al. (2017) and Moody et al. (2018), have presented evidence that informal sanctions can indeed exert a significant influence on compliance and may effectively encourage ISP compliance behavior. These divergent findings underscore the complexity of the relationship between informal sanctions and ISP compliance, suggesting that contextual factors and organizational dynamics may play a pivotal role in shaping the impact of informal sanctions.

In a nutshell, the acceptance of Hypothesis H4 signifies the significance of informal sanctions in fostering employees' intentions to comply with ISP. While previous research has generated mixed results, the positive relationship established in this study emphasizes the potential of informal sanctions as a valuable tool for promoting information security compliance within organizations. This nuanced understanding underscores the need for organizations to consider the contextual factors and organizational culture that may influence the effectiveness of informal sanctions in achieving robust ISP compliance.

5.2.5 Shame is positively related to employees' intention towards ISP compliance.

The acceptance of Hypothesis H5, asserting a positive relationship between "shame" and employees' intention towards ISP compliance, is supported by robust empirical evidence and contributes to our understanding of the complex interplay of emotions in shaping compliance behavior. Hypothesis H5, represented by the coefficient of the path "shame -> intention," is empirically substantiated by a statistically significant relationship (H5: $\beta = 0.200$; t-value= 4.223; $p < 0.01$) as evidenced in Table 5.1. This finding aligns with the proposed hypothesis, suggesting a positive association between shame and employees' intention towards ISP compliance.

Shame, as revealed in this study, exerts a positive effect on employees' intentions to comply with their organization's ISP. This result implies that when employees perceive noncompliance with information security policy as a shameful activity, they are more motivated to distance themselves from engaging in such behavior. This alignment with deterrence theory, which often includes shame as a self-imposed sanction, resonates with findings in criminology literature (Vance et al., 2020).

However, it's worth noting the discrepancy between this study's findings and a previous study by M. Siponen et al. (2010) in the field of information security. M. Siponen et al. (2010) reported an inability of shame to reduce employees' noncompliance to their organization's ISP. Similarly, a recent study by Vance et al. (2020) revealed that shame exerts a negative influence on employees' intention to violate an ISP, irrespective of cultural context. While a previous study in the field of information security examined the effect of shame on ISP violations, this research expands the understanding by investigating the impact of shame across different cultures.

A potential explanation for this contradiction could be rooted in the cultural makeup of the sample respondents in the above studies. This cultural distinction underscores the importance of considering cultural factors when examining the impact of emotions on compliance behavior. Vance et al. (2020) study supports this idea, and they claim that, to the best of their knowledge, no study, whether in information security or criminology, has previously explored the effect of shame on compliance behavior in such a cultural context.

Shame has been a subject of theoretical and empirical exploration in the fields of criminology and psychology. While some scholars in criminology have incorporated shame within the framework of deterrence theory, viewing it as a form of self-imposed sanction, others have questioned its fit within this theoretical framework, which traditionally revolves around calculated pain avoidance. Despite these debates, research on shame as a self-conscious emotion has flourished, highlighting its role in self-assessment and feelings of worthlessness, often stemming from a misalignment between self-evaluation and the ideal self-image.

Finally, the acceptance of Hypothesis H5 is founded on strong empirical evidence and contributes to the understanding of the role of shame in shaping employees' intentions regarding ISP compliance. This recognition of the universal impact of shame across cultures underscores its significance in the domain of information security policy adherence and provides valuable insights for organizations seeking to promote compliance behavior.

5.2.6 Consistency culture strengthens the positive effect between moral beliefs and compliance intention.

The acceptance of Hypothesis H6 contributes to a deeper understanding of the detailed interactions among "consistency culture," "moral beliefs," and "compliance intention." The study's results demonstrate how consistency culture influences the connection between moral beliefs and compliance intention. These findings offer valuable insights into the role of organizational culture in shaping employees' intentions regarding compliance with information security policies. Hypothesis H6, as presented in Table 5.1, posits that the presence of a consistency culture enhances the positive relationship between moral beliefs and the intention to comply. The aforementioned hypothesis has been substantiated through empirical evidence, demonstrating a statistically significant moderating effect (H6: $\beta = 0.086$; t-value= 2.446; $p < 0.05$).

The visual representation in Figure 5.2 depicts the interaction effect between moral beliefs and consistency on intention. The graph illustrates three distinct lines, each depicting the correlation between moral beliefs (represented on the x-axis) and ISP compliance intention (represented on the y-axis). The middle line symbolizes the correlation within a consistency culture of average level. The remaining two lines illustrate the association between the moderator variable, consistency culture, and higher (i.e., one standard deviation above the mean value of consistency culture) and lower (i.e., one standard deviation below the mean value of consistency culture) levels.

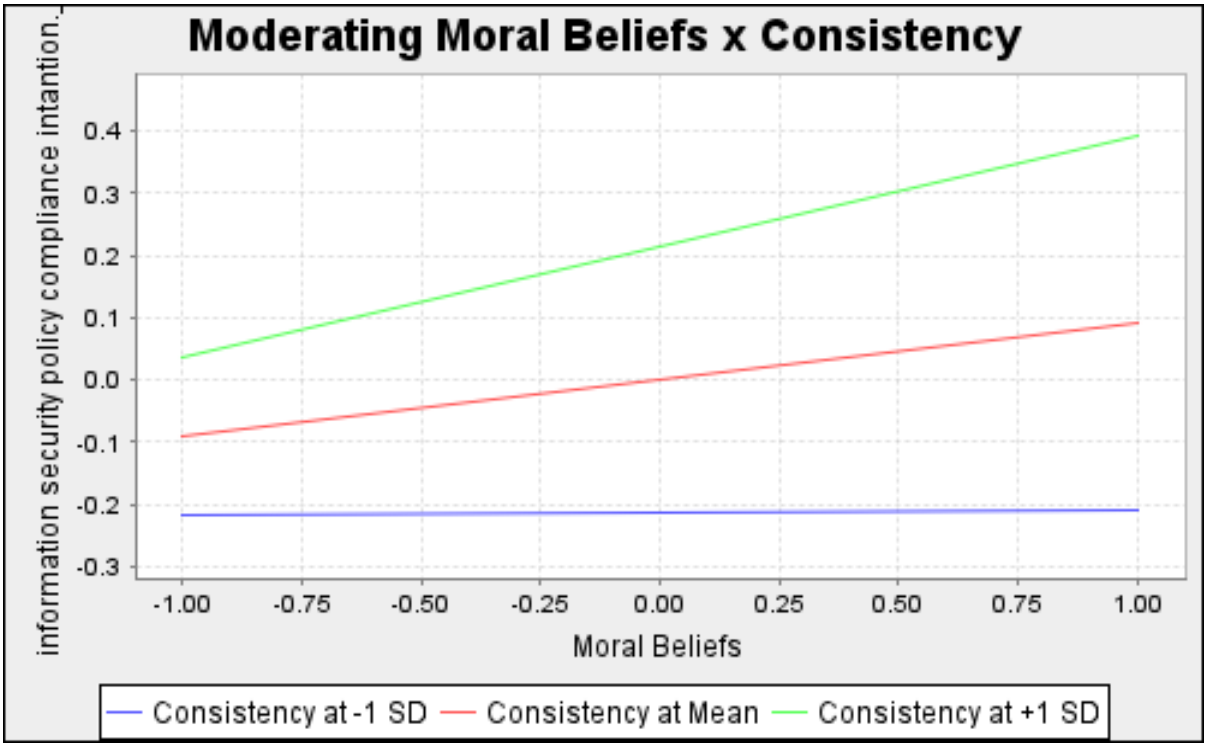


Figure 5. 2: The two-way interaction effect of moral beliefs x consistency on intention.

As illustrated in Figure 5.2, it is apparent that all three lines demonstrate a positive incline, thereby suggesting a positive correlation between moral beliefs and compliance intention. This suggests that there is a positive correlation between higher levels of moral beliefs and higher levels of compliance intention among employees.

Nevertheless, the crucial understanding arises from the moderation effect. At elevated levels of the moderator, namely consistency culture, there is a significantly heightened impact of moral beliefs on the intention to comply. In contrast, in cultural contexts characterized by lower levels of consistency, the influence of moral beliefs on the intention to comply becomes less pronounced. The present study highlights the influential role of organizational culture in shaping employees' behavioral intentions by examining the reinforcing impact of consistency culture on the positive association between moral beliefs and compliance intention. This study represents the initial empirical exploration of the moderating impact of consistency culture on the

association between moral beliefs and employees' compliance intentions, based on the current body of knowledge.

To sum up, the validation of Hypothesis H6 contributes to the advancement of our comprehension regarding the complex dynamics involving consistency culture, moral convictions, and the inclination to adhere to regulations within organizational contexts. The available empirical evidence substantiates the proposition that organizational culture, specifically consistency culture, has the potential to enhance the positive impact of moral beliefs on individuals' intentions to comply. The aforementioned discovery highlights the significance of adopting a coherent organizational culture in order to strengthen employees' dedication to adhering to ISP compliance. This, in turn, leads to improved information security measures within the organization.

5.2.7 Effectiveness culture strengthens the positive effect between perceived benefits and compliance intention.

The findings displayed in Table 5.1 and Figure 5.3 offer significant evidence in favor of Hypothesis H7, which suggests that the presence of an effectiveness culture enhances the positive relationship between perceived benefits and intention to comply. The hypothesis is supported by statistically significant results, indicating that the presence of an effectiveness culture is indeed important in strengthening the connection between perceived benefits and intention to comply.

The results of the moderation analysis, as presented in Table 4.15, demonstrate a significant moderating effect of effectiveness culture on the association between perceived benefits and compliance intention (H7: $\beta = 0.086$, $t = 3.359$, $P < 0.001$). The statistical significance of these findings highlights the credibility of Hypothesis H7, indicating that the presence of an effectiveness culture significantly affects the relationship between perceived benefits and compliance intention.

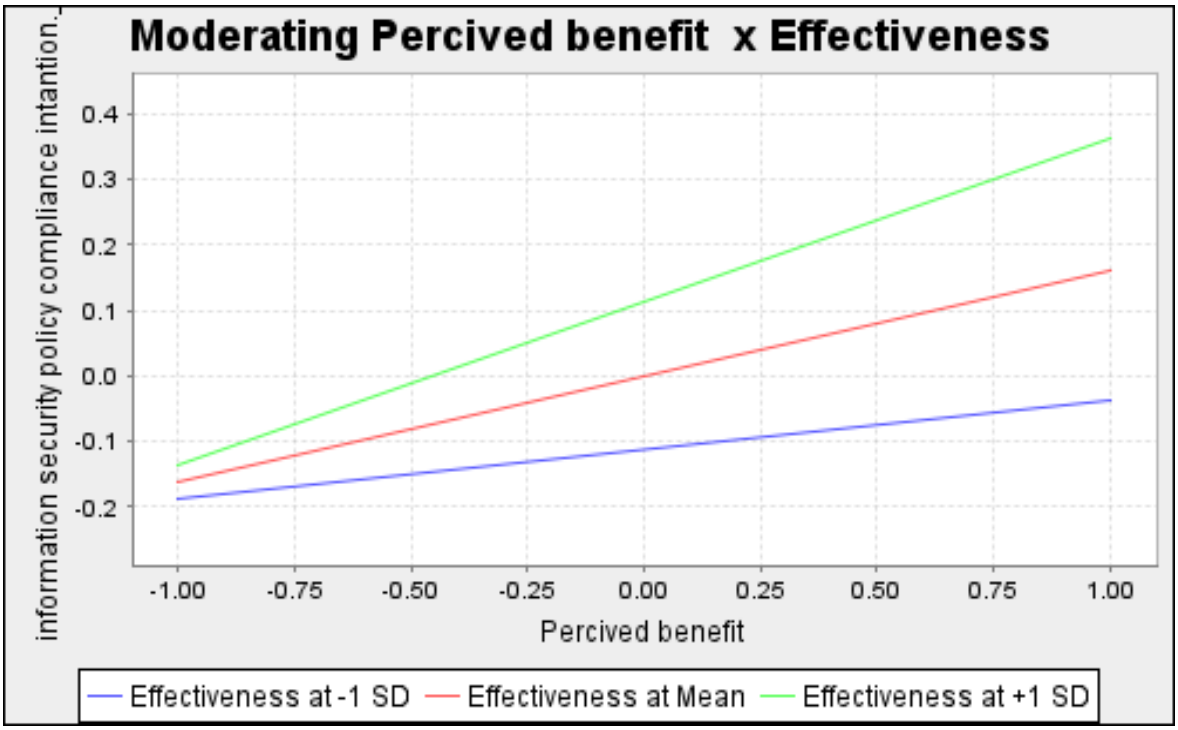


Figure 5. 3 : The two-way interaction effect of perceived benefits x consistency on intention.

To provide additional clarity on this correlation, Figure 5.3 presents a visual depiction of the reciprocal influence of perceived benefits and effectiveness culture on compliance intention. The diagram illustrates three separate lines that depict the correlation between different levels of effectiveness culture. The central line depicted in Figure 5.3 illustrates the correlation between perceived benefits and compliance intention under conditions where the level of effectiveness culture is moderate. Significantly, the observed trend in this line demonstrates a positive incline, suggesting that an increase in perceived benefits is associated with a greater inclination to comply, even when considering the average level of effectiveness culture.

Nevertheless, the importance of Hypothesis H7 becomes more evident when taking into account the lines that depict elevated and diminished levels of effectiveness culture. At elevated levels of effectiveness culture, there is a discernible amplification in the influence of perceived benefits on compliance intention. The aforementioned enhancement indicates that within organizational cultures that exhibit high levels of effectiveness, the perceived advantages linked to adherence to information security policies exert a more significant influence on employees' intentions to

comply. On the other hand, it can be observed that in contexts characterized by lower levels of effectiveness culture, the impact of perceived benefits on the intention to comply is somewhat diminished, as evidenced by the data point associated with a lower effectiveness culture score. This observation suggests that in organizational cultures that are less effective, the influence of perceived benefits on the intention to comply is less significant.

In conclusion, the results obtained from this research study offer substantial empirical evidence in favor of Hypothesis H7. The findings of this study provide evidence that an organizational culture focused on effectiveness does indeed enhance the positive association between perceived benefits and the intention to comply. The findings of this study provide significant contributions to the understanding of how organizational culture influences employees' intentions towards complying with information security policies. These results underscore the significance of incorporating cultural factors into the development of strategies aimed at fostering information security compliance within organizations.

Moreover, this research expands upon the current body of knowledge by examining the impact of an effectiveness culture on the relationship between perceived benefits and intention to comply, thereby enhancing our comprehension of these intricate dynamics within the realm of information security compliance.

5.2.8 Consistency culture strengthens the positive effect between formal sanctions and compliance intention.

Hypothesis H8 posits that a "consistency culture strengthens the positive effect between formal sanctions and compliance intention." This hypothesis finds substantial support in the empirical data presented in Table 4.15, where the moderating effect of consistency culture on the relationship between formal sanctions and compliance intention is statistically significant (H8: $\beta = 0.151$, t-value = 4.454, $P < 0.001$). Consequently, we can confidently accept H8, confirming that consistency culture indeed enhances the positive impact of formal sanctions on compliance intention.

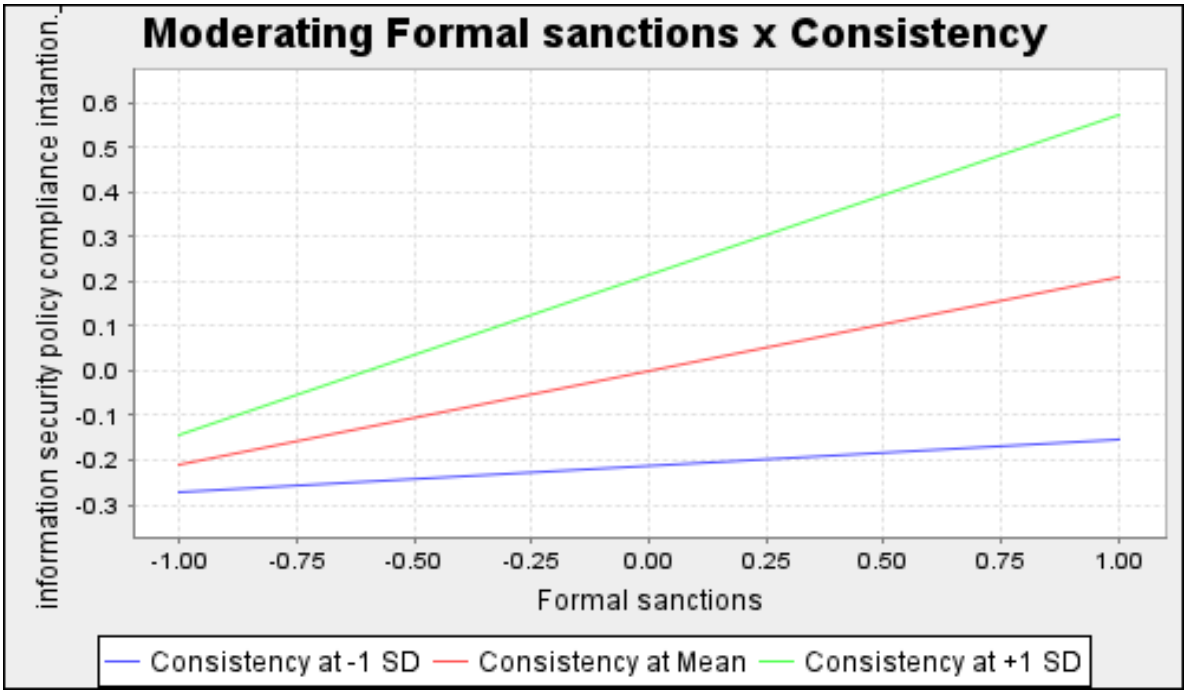


Figure 5. 4: The two-way interaction effect of formal sanctions x Consistency on Intention.

To provide a visual representation of this interaction, Figure 5.4 illustrates three distinct lines, each representing the relationship between formal sanctions (on the x-axis) and compliance intention (on the y-axis). The middle line corresponds to organizations with an average level of consistency culture. Additionally, there are two lines flanking the middle line, symbolizing scenarios with higher (i.e., one standard deviation unit above the mean value of consistency culture) and lower (i.e., one standard deviation unit below the mean value of consistency culture) levels of this cultural variable.

What becomes immediately apparent from Figure 5.4 is that all three lines exhibit a positive slope, indicating a positive relationship between formal sanctions and compliance intention. In simpler terms, the presence of formal sanctions tends to lead to higher levels of compliance intentions among employees. However, the strength of this relationship fluctuates depending on the prevailing level of consistency within the organization.

In settings characterized by a high consistency culture (as represented by the upper line in the graph), the impact of formal sanctions on compliance intention is notably more pronounced. In

such structured and rule-oriented environments, formal sanctions carry a heightened sense of legitimacy and efficacy. This means that employees within these organizations are more likely to recognize the consequences of non-compliance with information security policies, resulting in a stronger intention to comply. Conversely, in organizations with lower levels of consistency culture (as depicted by the lower line), the effect of formal sanctions on compliance intention is somewhat attenuated. In these less structured contexts, formal sanctions may exert a comparatively weaker influence on employees' compliance intentions.

A consistency culture emphasizes order, rules, regulations, uniformity, and efficiency, which is similar to formalized and regular organizations. Consistency-focused companies follow structured procedures, standard operating protocols, and established norms. Uniformity and consistency often lead to a highly regulated and rule-bound organization.

In contrast, formal sanctions are explicit penalties that deter specific organizational misconduct. These sanctions are central to deterrence theory, which uses punishment to deter bad behavior. Formal sanctions regulate non-compliance and misconduct. When considering their shared focus on structure, rules, and regulations. Organizations that value consistency naturally prefer well-defined processes and guidelines. The desire for order and regulation fits well with formal sanctions. In a consistency culture-driven organization, formal sanctions make non-compliance with rules and regulations clear and predictable. In such a culture, employees are more likely to anticipate and understand the consequences of information security violations. Thus, formal sanctions in this cultural context are more legitimate and effective.

In sum, the empirical findings, along with the inherent characteristics of consistency culture and formal sanctions, provide compelling evidence in support of Hypothesis H8. The structured and rule-bound nature of consistency culture aligns seamlessly with the principles of formal sanctions. Consequently, within a consistency culture-driven organization, formal sanctions are more likely to be perceived as legitimate and effective deterrents, thus reinforcing the positive impact of these sanctions on employees' compliance intentions. This underscores the critical importance of harmonizing organizational culture and formal sanctions to effectively promote compliance with information security policies.

5.2.9 Consistency culture strengthens the positive effect between informal sanctions and compliance intention.

5.2.10 Innovativeness culture strengthens the positive effect between Perceived benefits and compliance intention.

The empirical data does not provide support for Hypotheses H9 and H10, which suggest that "consistency culture enhances the positive relationship between informal sanctions and compliance intention" and "innovation culture enhances the positive relationship between perceived benefits and compliance intention," respectively.

According to the findings presented in Table 5.1, the statistical analysis reveals that there is no significant moderating effect of consistency culture on the relationship between informal sanctions and compliance intention (H9: β= -0.014, t-value = 0.510, P > 0.05). Therefore, it is necessary to refute H9, which posits that the Consistency culture does not exert a substantial reinforcing influence on the association between informal sanctions and the intention to comply. Likewise, in relation to H10, the empirical examination presented in Table 5.1 reveals that the influence of Innovativeness culture on the association between Perceived benefits and compliance intention is not statistically significant (H10: β= 0.044, t-value = 1.646, P > 0.05). Thus, we can conclude that H10 is rejected, suggesting that the presence of an innovativeness culture does not have a substantial enhancing effect on the association between Perceived benefits and compliance intention.

In brief, the research results fail to provide evidence in favor of the proposition that consistency culture enhances the favorable impact of informal sanctions on compliance intention (H9) or that innovativeness culture strengthens the positive influence of perceived benefits on compliance intention (H10). The aforementioned hypotheses, although theoretically viable, do not correspond with the empirical evidence, thereby emphasizing the intricate and multifaceted role of organizational culture in shaping outcomes related to compliance.

5.2.11 Cooperativeness culture strengthens the positive effect between shame and compliance intention

Hypothesis H11 postulates that "cooperativeness culture strengthens the positive effect between shame and compliance intention." The empirical analysis, as presented in Table 5.1, provides support for H11, indicating that cooperativeness culture indeed plays a significant role in enhancing the positive relationship between shame and compliance intention. Figure 5.5 visually represents the dynamics of this relationship, using three distinct lines to illustrate the connection between shame (x-axis) and compliance intention (y-axis). The middle line represents the scenario for an organization with an average level of cooperativeness culture. The other two lines depict the relationship between shame and compliance intention in situations where cooperativeness culture is either higher (i.e., one standard deviation unit above the mean) or lower (i.e., one standard deviation unit below the mean).

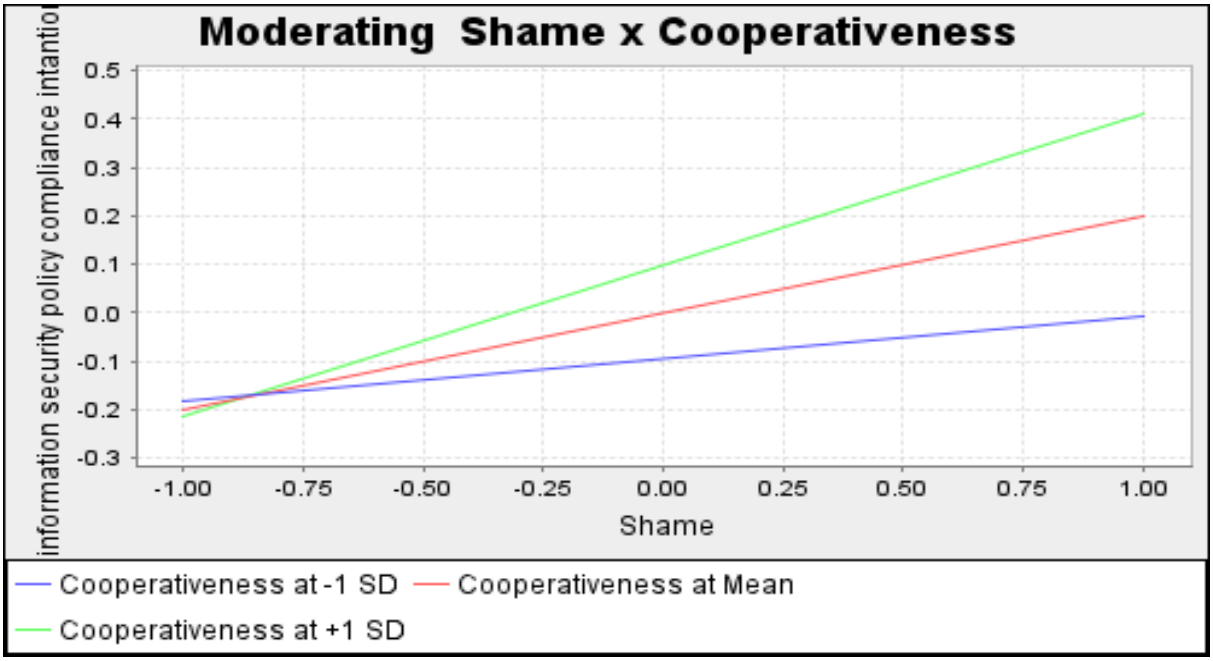


Figure 5. 5: The two-way interaction effect of shame x Consistency on Intention.

From the graphical representation in Figure 4.6, it becomes evident that all three lines exhibit a positive slope, indicating that higher levels of shame are associated with higher levels of

compliance intention. This initial observation aligns with the theoretical premise that shame acts as a deterrent to socially undesirable actions, including non-compliance with organizational policies and regulations.

However, it is through the lens of cooperativeness culture that the true impact of shame on compliance intention is unveiled. The empirical data confirm that, due to a positive moderating effect, when an organization possesses a high level of cooperativeness culture, the influence of shame on compliance intention is notably stronger. In contrast, when the cooperativeness culture is less pronounced within the organization, the effect of shame on compliance intention is comparatively weaker. This distinction emphasizes the significant role played by the organizational culture in amplifying or attenuating the impact of shame as a driver of compliance intention.

Cooperativeness culture, characterized by its emphasis on cooperation, information sharing, trust, empowerment, and teamwork, creates an environment where individuals are more inclined to respond positively to feelings of shame or guilt associated with non-compliance. In such a culture, the cooperative and team-oriented atmosphere fosters a sense of collective responsibility, wherein individuals are motivated to uphold organizational standards and exhibit behaviors aligned with compliance. The relationship between cooperativeness culture and shame finds support in the broader deterrence literature, which acknowledges that shame, akin to formal sanctions, can serve as a powerful mechanism for deterring individuals from engaging in undesirable actions. Research in the field of deterrence (Grasmick and Bursik, 1990; Nagin and Paternoster, 1993; D’Arcy et al., 2011) underscores the role of shame in reducing undesirable behaviors, reinforcing the idea that shame can effectively deter individuals from violating organizational policies when situated within a cooperativeness culture.

In conclusion, the acceptance of Hypothesis H11 highlights the pivotal role of cooperativeness culture in strengthening the positive effect of shame on compliance intention. This finding underscores the significance of organizational culture in shaping individuals' responses to feelings of shame and emphasizes the importance of fostering a cooperative and supportive cultural environment to enhance compliance with organizational policies and regulations.

In this section, the results of the control variables are presented, shedding light on their influence on employees' compliance intentions. Table 5.1 provides a summary of these results, including path coefficients, statistical tests, and p-values, which are essential for assessing the significance of these variables.

Path	Beta	T Statistics	P Values	Results
Gender -> Intention	0.074	3.055	0.002	Significant
Age -> Intention	0.029	1.180	0.238	Not Significant
Scenario types -> Intention	-0.001	0.051	0.959	Not Significant

Table 5. 2 Results of control variables

The control variables examined in this study encompassed gender, age, and scenario types. Their impact on employees' compliance intentions was systematically analyzed, yielding the following outcomes: Gender -> Intention: The analysis revealed a statistically significant relationship between gender and compliance intentions. Specifically, the path coefficient (Beta) for gender was found to be 0.074, with a corresponding t-value of 3.055 and a p-value of 0.002 as demonstrated by the data presented in Table 5.2.

This outcome suggests that gender plays a significant role in influencing employees' intentions toward compliance with information security policies. Age -> Intention: Conversely, the analysis demonstrated that age did not exert a significant impact on employees' compliance intentions. The path coefficient for age was 0.029, with a t-value of 1.180 and a p-value of 0.238. These results indicate that age is not a decisive factor in shaping employees' intentions regarding information security policy compliance. Scenario Types: -> Intention: Similarly, the examination of scenario types revealed that they had no significant influence on employees' compliance intentions.

The path coefficient for scenario types was found to be minimal, at -0.001, with a negligible t-value of 0.051 and a p-value of 0.959. Consequently, the type of scenario presented did not meaningfully impact employees' intentions regarding compliance with information security policies. In summary, the results of the control variables analysis elucidate the varying degrees

of influence these factors exert on employees' compliance intentions. While gender was identified as a significant determinant, age and scenario types were found to be non-significant in this context. These findings contribute to a more nuanced understanding of the multifaceted factors that can shape compliance intentions within organizational settings.

5.3 Summary of Findings and Discussion

In this chapter, each hypothesis concerning employees' intentions towards ISP compliance was thoroughly examined and discussed. The hypothesis testing phase rigorously assessed H1 through H11, shedding light on various factors influencing organizational compliance intentions.

Beginning with H1, the results strongly affirmed a positive correlation between employees' moral beliefs and their intentions to comply with ISP regulations. This finding aligns with RCT and corroborates existing criminological and psychological research, highlighting the pivotal role of moral reasoning in fostering desirable behaviors.

Moving on to H2, the analysis substantiated that the presence of formal sanctions increases employees' intentions to comply with ISP regulations. This underscores how explicit penalties act as a deterrent to non-compliance and serve to promote adherence to ISP protocols within organizations.

Similarly, H3 found empirical support, revealing that employees' perception of the benefits associated with compliance positively influences their intentions to comply with ISP regulations. This suggests that emphasizing the advantages of compliance may effectively enhance employees' commitment to adhering to ISP guidelines.

Furthermore, H4 demonstrated a positive relationship between informal sanctions and employees' compliance intentions, emphasizing the significance of informal mechanisms in fostering compliance within organizational settings.

Regarding H5, the analysis confirmed that the experience of shame serves to increase employees' intentions to comply with ISP regulations, indicating that feelings of shame act as a deterrent against ISP violations.

H6 elucidated that organizational cultures emphasizing consistency and orderliness bolster employees' moral beliefs and intentions to comply with ISP regulations, highlighting the role of cultural norms in shaping compliance behavior.

However, H7 did not find empirical support, indicating that an organizational culture focused on effectiveness does not significantly strengthen the relationship between perceived benefits and compliance intentions.

On the other hand, H8 received strong empirical support, demonstrating that consistency-oriented cultures enhance the effectiveness of formal sanctions in promoting compliance among employees.

H9 and H10, concerning the effects of consistency and innovativeness cultures on informal sanctions and perceived benefits, respectively, did not receive empirical support, suggesting that these culture types do not significantly influence compliance intentions.

Lastly, H11 found substantial support, indicating that a cooperative organizational culture enhances the effectiveness of shame as a deterrent against non-compliance.

In the subsequent chapter, the practical and theoretical implications of these research findings will be thoroughly discussed, concluding with actionable recommendations derived from the study's insights.

CHAPTER SIX: CONTRIBUTIONS, DELIMITATIONS AND IMPLICATIONS

6.1. Introduction

In the preceding chapter, data validation and data analysis procedures were carried out, subsequently leading to a comprehensive examination of the primary research findings. This chapter presents a comprehensive examination of several key areas. Firstly, it provides a summary of the research questions that were initially introduced in the preceding chapter, along with a detailed analysis of the major methodologies employed to address these questions. Additionally, it outlines the significant contributions that this study has made to the fields of research, theory, and practical application. Furthermore, the chapter critically evaluates the primary limitations of the study and explores the potential implications that this research may have for future investigations. Finally, a concluding remark is offered to summarize the overall findings and insights of the study.

6.2. Research Questions Revisited

Despite periodic increases in the frequency and cost of breaches within the information security caused by insiders, significant efforts have been made to address this issue from behavioral perspectives. Culture is a significant yet understudied factor in relation to compliance with information security policy from a behavioral perspective (Tilahun and Tibebe, 2017).

In the African context, there is limited knowledge regarding the precise influence of organizational culture on employees' compliance behavior with information security policies. Previous research conducted in western culture has produced varied results regarding the influence of organizational cultural dimensions on individuals' compliance behavior with information security policies (Arage et al., 2015; Doupnik and Tsakumis, 2004). It is worth noting that none of these studies have examined culture at the individual level (Arage et al., 2015). Furthermore, a significant number of empirical studies have been conducted to examine individuals' information security behavior.

These studies primarily employ the protection motivation theory and/or the general deterrence theory. However, it is worth noting that these studies predominantly emphasize fear-based strategies and offer only limited insights (Vance and Siponen, 2012). In contrast, the rational choice theory approach incorporates supplementary constructs such as moral beliefs and perceived benefits, which contribute to a comprehensive understanding of the issue of information security (Li et al., 2010). In this context, a limited number of studies conducted in western settings, for example (Li et al., 2010; M. Siponen et al., 2010; Vance et al., 2012) have employed certain constructs of the rational choice theory to examine individuals' compliance behavior with information security policies. These studies have yielded inconsistent and occasionally conflicting results when compared to previous research on the general deterrence theory (D'Arcy and Herath, 2011). Therefore, further research is needed to examine the generalizability of these findings to various organizational cultures.

Upon reviewing the limited existing studies that have explored the influence of organizational culture and rational choice theory constructs on employees' compliance behavior with information security policies in economically developed countries, several deficiencies were identified. First, based on the available literature, it appears that none of the studies conducted have measured organizational culture at the individual level or empirically examined the potential moderating impact of organizational culture in the context of information security policy compliance. Second , the construct of shame in the context of rational choice theory has received limited attention in research, with only known study by M. Siponen and Vance (2010) and Vance et al. (2020) exploring its impact on employees' compliance with information security policies.

Furthermore, there is a lack of investigation into all the constructs of RCTs within the context of low-income countries, specifically in the African context. Third, none of the previous studies have examined the moderating influence of organizational culture within economically developing countries, specifically in the African region. Fourth, in the context of developing economies, the existing research generally lacks comprehensive explanations regarding the factors influencing compliance with the Information Security Policy compliance.

As a result, in order to address the gaps that were left by earlier research, we developed the following research questions in the first chapter: research question one: How do formal sanction, informal sanction, perceived benefits, moral beliefs, and shame affect employees' intention to comply their organization's information security policy? research question two, How does organizational culture moderate the effect of formal sanctions, informal sanction, perceived benefits, moral beliefs, and shame on employees' intention to comply their organization's information security policy?. Hence, in the following subsections, we will provide a summary of how this study responded to the two research questions that were posed.

How do formal sanction, informal sanction, perceived benefits, moral beliefs, and shame affect employees' intentions to comply with their organization's information security policy?

To investigate the research question at hand, an extensive literature review was conducted to examine the constructs associated with rational choice theory. In this context, we have examined and deliberated upon various research endeavors pertaining to each of the constructs of rational choice theory and their correlation with the information security behavior exhibited by employees (refer to Section 2.4). Within this particular section, we also engaged in a discourse regarding the constraints inherent in the existing research pertaining to the phenomenon of information security. Our analysis reveals a dearth of knowledge regarding the influence of shame, formal sanctions, informal sanctions, perceived benefits, and moral beliefs on employees' intention to comply with their organization's ISP in the context of developing countries.

Furthermore, we provided a rationale for the distinct methodological approach employed in the study, as detailed in chapter 3. Following the administration of validity and reliability tests on the survey instruments, the hypotheses were subsequently examined utilizing survey data obtained from organizations that possess established information security policy. Based on the empirical evidence presented in the study, it was observed that moral beliefs, perceived benefit, formal sanctions, informal sanctions and shame have a significant impact on employees' inclination to comply with their organization's information security policy. The findings of this study align with previous research conducted in the fields of information security and

criminology. For instance, (Arage et al., 2015; M. Siponen et al., 2010; Vance et al., 2020) have all reported similar results.

In line with our study's focus on the impact of moral belief, it's noteworthy to consider the findings of a related study. In their research, M. Siponen et al. (2010) and Vance et al. (2020), they found that moral belief had a negative influence on the intention to violate rules, indicating that individuals who saw the violation of a specific rule as morally wrong reported a decreased intention to break that rule. This aligns with our own findings, which demonstrate that moral belief indeed has a positive influence on the intention to comply with the ISP.

In our model, moral belief emerges as the strongest factor, supporting the notion that individuals who view a certain behavior as morally right are more inclined to abide by it. Furthermore, it was observed that employees were motivated to comply with their organization's Information Security Policy due to the perceived advantages associated with compliance. In examining the impact of shame on employees' intentions to comply with information security policies to contextualize our research, we draw upon existing literature that has explored the relationship between shame and ISP. Previous studies have consistently shown that shame plays a pivotal role in discouraging employees from violating Information security policies. Previously, only two study in the field of has examined the effect of shame on ISP namely Vance and Siponen (2010) and Vance et al. (2020).

However, to the best of our knowledge, no study, whether in information security or criminology, has examined the effect of shame on organizational culture; instead, these studies have examined shame in the context of notional culture (Arage et al., 2015; Elis and Simpson, 1995; Grasmick and Bursik Jr, 1990; Nagin and Paternoster, 1993; Raymond Paternoster and Simpson, 1996). Employees who experience shame as a result of potential policy violations are less motivated to engage in risky behavior, as they actively seek to avoid the negative emotional consequences associated with shame. Moreover, these findings have suggested that shame can also positively influence compliance by reinforcing the importance of compiling to information security policies. This finding aligns with previous research conducted by M. Siponen et al. (2010), Li et al. (2010), Vance et al. (2012); Vance and Siponen (2012) and Vance et al. (2020). Hence, this

study effectively addresses the initial research question that was presented at the outset of the investigation.

How does organizational culture moderate the effect of formal sanctions, informal sanctions, perceived benefits, moral beliefs, and shame on employees' intention to comply their organization's information security policy?

To answer this research question, first and foremost, we made a detailed overview of organizational culture (see section 2.7.1) and a brief analysis of the current literature about the influence of organizational culture on different types of IT related issues (see section 2.8). Particularly, we reviewed research works that mainly focus on how each of the organizational culture dimensions are related to the information security behavior of individuals (see section 2.7.2 and section 2.8). Moreover, we also discussed the shortcomings of studies that investigate the impact of organization culture on individuals' ISB (see section 2.8). In this regard, our review showed that there exists hardly any research that investigate the moderating impact of organizational culture dimensions on employees' intention to comply with their organization information security policy.

In the third chapter, we discussed the philosophical position of the study and prepared the survey instruments related to the four dimensions of organizational culture, while in the fourth chapter, we conducted validity and reliability tests on the instruments. Finally, the hypotheses that proposed the moderating influence of organizational culture were tested using a survey data collected from organizations that do have established ISP (see chapter 4).

The output of the empirical test indicates that nine out of 11 hypotheses were supported by the collected data. More specifically, the impact of perceived benefits, formal sanctions, shame, and moral beliefs on employees' intention to comply with their organization information security policy was found to be moderated by consistency, effectiveness and cooperativeness culture (see Table 4. 13). In this respect, our findings are consistent with prior studies that were conducted in different area, such as; Hofstede (2001, 2003, 2011) in the area of sociology; Timo (2009) in the area of ISS; Doupnik and Tsakumis (2004) in the area of finance.

Generally, we believe that this study has identified some of the determinants of employees' intention to violate their organizations ISP, and hence both of the research questions are sufficiently addressed.

6.3 Study implications

This study aims to examine and analyzes the key factors that are hypothesized to influence employees' intentions to comply with their organization's information security policy. These factors have been identified, discussed, and empirically tested in order to determine their direct or moderating effects. In this study, we conducted a comprehensive examination of existing literature on the factors influencing employees' compliance behavior with information security policies compliance. We applied relevant theoretical frameworks to conceptualize these determinants and subsequently conducted empirical testing within the Ethiopian context. It is worth noting that this region has been overlooked in previous research on information security compliance in Sub-Saharan Africa. The research framework utilized in this study was developed by incorporating elements of organizational culture and rational choice theory. This study has made significant contributions to the fields of research, practice, and theory. In the subsequent sections, we will elaborate on these contributions extensively.

6.3.1 Theoretical implication

From a theoretical viewpoint, the implications are manifold. First, this study offers a holistic view of ISP compliance behaviors by developing a model using the RCT and CVF theories. Our research findings indicate that a comprehensive analysis of the impact of deterrent countermeasures necessitates the inclusion of organizational cultural dimensions. The examination of employees' compliance with information security policies necessitates a holistic approach that integrates deterrent countermeasures with organizational culture. This integration could potentially shed light on the inconsistent results observed in previous research regarding the influence of deterrent countermeasures on information security policies compliance.

In this context, based on current understanding, this research represents the initial examination of the role of organizational culture in moderating the relationship between RCT constructs and

employees' intention to comply with their organization's information security policies. There is a limited body of research, for instance (Butler and Brown, 2023; Ernest Chang and Lin, 2007; Hu et al., 2012; Karlsson et al., 2022; Tang et al., 2016), that has attempted to incorporate the understanding of organizational culture within the domain of information security. However, none of these studies have conducted empirical tests or explored the moderating impact of organizational culture. Therefore, our research has made a novel contribution by examining the moderating influence of various dimensions of organizational culture (consistency, cooperativeness, effectiveness, and innovativeness) on employees' intentions to comply with their organization's ISPs. Furthermore, the discovery presented in this study holds significant implications for research in the field of information security. It highlights that compliance to ISP is influenced not only by the fear of sanctions, but also by moral beliefs and perceived benefits.

Secondly, Hofstede (2001) discusses the concept of organizational culture, specifically referring to groups such as organizations or different functional units within an organization in Professor Hofstede's definition of organizational culture. Nevertheless, this research specifically assesses the individual-level measurement of organizational culture. One of the criticisms directed towards Hofstede's (2001) cultural dimension can be addressed by employing the method commonly utilized in information security research. There exists a viewpoint among certain scholars that the utilization of Hofstede's cultural dimensions in the context of organizations might result in an oversimplification of the complex nature of organizational culture (Sndergaard, 1994).

One of the primary critiques that have been raised regarding Hofstede's research is centered on this particular aspect. There exists a viewpoint among certain individuals that Hofstede's dimensions fail to widely encompass the entirety of cultural differences that may be present within a given organization and its diverse subcultures (Triandis, 2001). Consequently, we hold the viewpoint that this may serve as a catalyst for researchers engaged in the field of information security to reassess their investigations pertaining to culture by adopting an individual-level approach to measure organizational culture. To the best of our knowledge, there is currently a lack of research in the field of information security that examines and utilizes organizational culture at the individual level. The aforementioned work constitutes a significant and pioneering

addition to the existing corpus of empirical investigations within the realm of information security.

Third, this study adds value to the advancement of commutative theories by integrating distinct theoretical frameworks on information security compliance behaviors. Specifically, it introduces a novel model that incorporates the non-fear-based deterrence theory, referred to as the RCT, and the organizational cultural theory, known as the CVF. As previously stated, this research makes a significant contribution in this regard. The model was constructed based on the foundation provided by these two theories. The empirical test outcome further substantiates the appropriateness of integrating these two theories, thereby offering supplementary perspectives on the issue of employees' compliance with information security policies.

Lastly, this study offers a significant contribution by examining the varying effects of shame, moral beliefs, formal and informal sanctions and perceived benefits across different levels of organizational culture dimensions. By doing so, it addresses a gap in the existing literature, shedding light on important factors that have been neglected in previous research. This finding may serve as a catalyst for future researchers to investigate significant variables that have received limited attention in the realm of employees' compliance behavior with information security policies.

6.3.2 Practical implications

The study's findings not only contribute to existing theoretical knowledge but also offer valuable insights for practical implementation. Initially, it is essential for information security managers and policy makers to acquire significant knowledge regarding the mitigating influence of various elements of organizational culture on employees' intention to comply with their organization's information security policy. The INSA is the designated entity in Ethiopia responsible for the development and implementation of information security policy initiatives on a national scale. Regrettably, the INSA has implemented an information security policy framework that appears to have been replicated directly from ISO 27002. Consequently, organizations in Ethiopia are required to comply with the information security policy standards outlined in International

Standard Organization 27002 without any modifications. The existing standards in the domain of information security, namely ISO/IEC 27002 and ISO/IEC 27001, and Baseline Protection Manual, exhibit a significant oversight regarding the influence of culture on information security, as highlighted by Timo (2009).

This is in contrast to the existing literature, which suggests that culture significantly impacts the dissemination and adoption of diverse practices, including those related to information technology (Bjorck and Jiang, 2006). Ifinedo (2009) asserts that national and organizational culture significantly impact the successful implementation of foreign practices (Ifinedo, 2009). When considered from this perspective, the results of this study will provide significant support to the policymakers at information network security agency who are involved in the decision-making process regarding the adoption or modification of the current information security policy. The subsequent points encompass several significant implications for policymakers and managers tasked with formulating information security policies.

One key finding of this study reveals a significant and positive correlation between higher levels of moral beliefs and an increased intention to comply with rules and regulations. This relationship highlights the pivotal role that an individual's moral compass plays in shaping their commitment to adhering to ethical and regulatory standards. However, what makes this relationship even more intriguing is the presence of a moderating factor, known as consistency culture. This moderating factor has a notable influence on the connection between moral beliefs and compliance intention. Specifically, it amplifies the impact of moral beliefs on compliance intention when consistency culture is at a higher level.

In essence, organizations or contexts characterized by a strong emphasis on consistency culture tend to strengthen the bond between moral convictions and the intention to comply with rules and regulations. Conversely, when consistency culture within an organization or context is at a lower level, the effect of moral beliefs on compliance intention is comparatively weaker. This observation underscores the critical role that organizational culture, particularly one of consistency, plays in shaping the dynamics of ethical behavior and compliance intention. In conclusion, the presence of a consistency culture serves as a reinforcing mechanism, bolstering

the positive relationship between moral beliefs and the intention to comply with rules and regulations. It underscores that within environments where consistency culture is prevalent, individuals are more inclined to translate their moral convictions into concrete actions aligned with compliance, thus demonstrating a stronger commitment to ethical conduct. These insights hold valuable implications for organizations aiming to cultivate and sustain a culture of compliance and ethics within their operational frameworks.

Another noteworthy observation from this study is the presence of a positive moderating effect, which significantly influences the relationship between perceived benefits and compliance intention. This moderating effect becomes more pronounced when the level of the moderator, namely, effectiveness culture, is higher. In other words, organizations or contexts with a strong emphasis on effectiveness culture tend to amplify the impact of perceived benefits on compliance intention. Conversely, when the effectiveness culture within an organization or context is at a lower level, the effect that perceived benefits have on compliance intention tends to be comparatively weaker.

This finding underscores the role of effectiveness culture as a crucial contextual factor that shapes the dynamics between perceived benefits and compliance intention. In essence, the presence of an effectiveness culture serves to reinforce and strengthen the positive relationship between moral beliefs and compliance intention. It signifies that within environments where effectiveness culture is prominent, individuals are more likely to be swayed by the perceived benefits associated with compliance, thereby making them more inclined to adhere to ethical and regulatory guidelines. This nuanced understanding of the interplay between these factors sheds valuable light on the complex dynamics governing compliance intention and highlights the pivotal role of organizational culture in shaping ethical behavior. These findings offer important insights for organizations seeking to foster a culture of compliance and ethics within their operations.

An additional intriguing discovery arising from this study is the presence of a notable moderating effect that significantly influences the relationship between formal sanctions and compliance intention. This moderation effect becomes particularly pronounced when the level of the

moderator, namely, consistency culture, is at its zenith. In such contexts, where consistency culture is strongly embedded, the impact of formal sanctions on compliance intentions is notably more potent. Conversely, when consistency culture within an organization or context is at a lower level, the effect of formal sanctions on compliance intention tends to be comparatively subdued.

This finding underscores the pivotal role played by consistency culture as a contextual factor that shapes the dynamics between formal sanctions and the intention to comply. In essence, the presence of a robust consistency culture serves as an augmenting force, enhancing the positive relationship between formal sanctions and compliance intention. It implies that in environments where consistency culture is prevalent, individuals are more inclined to perceive formal sanctions as effective deterrents, thus strengthening their commitment to comply with rules and regulations.

This observation carries significant implications for organizations seeking to bolster their compliance frameworks. Understanding the amplifying role of consistency culture can guide the strategic implementation of formal sanctions as a means to foster a culture of adherence and ethical behavior. In such environments, formal sanctions are more likely to be perceived as a compelling mechanism for promoting compliance, ultimately contributing to a stronger commitment to ethical conduct and regulatory compliance.

Furthermore, one of the significant findings emerging from this study is the presence of a noteworthy moderating effect that significantly shapes the relationship between the emotion of shame and compliance intention. This moderating effect becomes particularly pronounced when the level of the moderator, referred to as the cooperativeness culture, is at its peak. In such organizational or contextual settings where the cooperativeness culture is strongly entrenched, the influence of shame on compliance intention is notably more robust and pronounced.

Conversely, when the level of cooperativeness culture within an organization is low, the impact of shame on compliance intention tends to be less potent. This observation underscores the pivotal role that cooperativeness culture plays as a contextual factor in melding the dynamics between the emotion of shame and the intention to comply with rules and regulations. In essence,

a thriving and highly cooperative culture serves as an augmenting force, amplifying the positive connection between experiencing shame and the intention to comply. This suggests that within environments characterized by a strong cooperativeness culture, individuals are more likely to respond to feelings of shame by demonstrating a heightened commitment to complying with ethical and regulatory standards.

These insights have profound implications for organizations aiming to foster a culture of compliance and ethical conduct. Recognizing the reinforcing role of cooperativeness culture can guide strategic efforts to address and harness the influence of shame as a driver of compliance. In such cooperative environments, the emotional response of shame is more likely to be leveraged as a motivational force, ultimately enhancing the commitment to ethical behavior and regulatory compliance.

In relation to the process of formulating policies, although not the primary focus of this study, the preliminary findings indicate that a significant number of organizations in Ethiopia, including those in the private and public sectors, do not possess a standardized information security policy. It is noteworthy to mention that in Ethiopia, the information network security agency (Harvey et al.), serves as the authorized entity entrusted with the formulation and implementation of information security policies at the national level.

In light of the apparent deficiencies in information security protocols observed in Ethiopian establishments, it is imperative for businesses and governmental bodies to accord high importance to the formulation and execution of comprehensive information security policies at both the organizational and departmental levels. Close collaboration with the INSA in order to align with national initiatives has the potential to greatly enhance the effectiveness of information systems and bolster data protection measures. The implementation and enforcement of standardized information security policies are crucial to ensuring the protection of sensitive information and the efficient mitigation of potential risks.

Issues related to awareness of information security policies. Awareness of information security policies is a critical aspect of ensuring the protection and confidentiality of sensitive data within

an organization. However, there are several issues that can hinder the effectiveness of information security policy awareness efforts. It is imperative for information security managers to develop comprehensive security training, awareness, and education initiatives that foster a culture wherein employees prioritize adherence to organizational information security policies over personal or work-related interests. According to previous research conducted by Puhakainen (2006), certain employees may perceive adherence to these policies as an obstacle to their operational efficiency. Hence, it is imperative for initiatives focused on security education and awareness to actively attempt to alter this perspective. Furthermore, it is crucial to underscore the significance of organizational culture in influencing employees' attitudes towards information security and their level of adherence to policies.

As indicated in the preceding paragraphs, the implementation of effective security education, training, and awareness programs is crucial for acquainting employees with various Information Security policy concerns. The utilization of scenario-based training programs has been identified as a crucial mechanism contributing to the effectiveness of these programs (Puhakainen, 2006). As per the author's assertion, this category of programs has demonstrated efficacy in effectively conveying to employees the potential consequences that a company may encounter as a result of security rule violations.

In this regard, it is imperative for organizations to establish a follow-up mechanism in order to assess the efficacy of their security education, training, and awareness initiatives. Organizations have the ability to utilize feedback and evaluation mechanisms in order to gain insight into the level of communication and comprehension of security objectives among employees. This is particularly significant as it enables managers responsible for information security to separate the effectiveness of various mechanisms and identify areas that require further enhancement (Wilson and Hash, 2003).

The Impact of Gender on Intention: The observation that gender exerts a substantial influence on intention is of considerable importance from a practical standpoint. This suggests that when developing interventions for information security policy compliance, organizations and policymakers should take into account gender-based disparities. For instance, the efficacy of

tailored training programs or awareness campaigns could be enhanced by incorporating considerations of gender-specific factors that impact individuals' inclination to comply. The acknowledgment of gender-based differentiations has the potential to facilitate the development of more focused and effective approaches aimed at enhancing adherence within the labor force.

The Influence of Age as an Insignificant Variable: The lack of a statistically significant relationship between age and intention indicates that, within the specific parameters of this study, age does not exert a significant influence on employees' intention to comply with ISP regulations. This information holds practical implications for organizations with regards to the allocation of resources. The necessity of prioritizing age-specific interventions for compliance may be called into question, as it may be more effective to allocate resources towards other factors such as moral beliefs or perceived benefits.

The lack of significance in the impact of scenario types on intention suggests that the particular scenarios employed in the study do not exert a substantial effect on employees' inclination to comply with ISP regulations. This information possesses practical implications for future research, indicating that the inclusion of scenario types may not hold significant importance in the design of experiments or surveys pertaining to compliance intention within this particular context

The incorporation of control variables and the examination of their statistical significance exemplify a comprehensive methodology for comprehending the determinants influencing individuals' intentions to comply. This methodology holds significant value in practical decision-making scenarios, where numerous factors have the potential to impact the final results. Organizations and policymakers can derive advantages from adopting a comprehensive viewpoint by taking into account a range of factors that could potentially influence individuals' inclination to comply, and subsequently customizing their approaches in response.

The inclusion of these control variable findings in your dissertation serves to enhance the validity of your research and offers valuable insights for both organizations and policymakers. This statement underscores the significance of taking into account gender-related variables in

compliance interventions, questions the need for age-specific strategies, and suggests that scenario types have a minimal impact on compliance intention. The aforementioned findings have the potential to contribute valuable insights towards the development of enhanced strategies aimed at fostering compliance with information security policies in practical settings.

6.4 Study Limitations

There are some limitations of this study that deserve mentioning so that researchers can consider them when replicating this study or studying information security behavioral aspect in general. These limitations need to be evaluated with the understanding that this study is the first of its kind in the specific domain of information security to scope out the phenomenon with this breadth and width.

One notable limitation worth considering is the absence of a direct measure of employees' actual behavior. Instead, this study relies on employees' intentions as the dependent variable, leading to the question of whether intention truly reflects employees' real-world actions. Many researchers, however, advocate for the use of intention as a valuable approximation that effectively explains behavior. The psychological theory of planned behavior, as proposed by Ajzen (1991), suggests that people often behave in line with their predictions. In support of this approach, researchers such as Paternoster and Simpson (1996), Wenzel (2004), Pahnila et al. (2007), and Siponen and Vance (2010) have employed intention as a proxy to predict employees' workplace behavior.

Another limitation of this study pertains to the selection of companies solely based on the presence of a well-established information security policy. We specifically included organizations in our sample by consulting their information security officers to confirm the existence of a documented and communicated information security policy (appendix III CBE ISP), while excluding those without such policies. This selection criterion could potentially raise questions about the representativeness of the chosen organizations. However, it was imperative for this study to focus on employees operating within an information security policy framework, as conducting research on those without such policies would not have been feasible.

Furthermore, it's worth noting that previous studies in the field of information security have adopted similar procedures (e.g., Li et al., 2010; Vance and Siponen, 2012).

Moreover, due to the sensitive nature of the study topic, respondents may be inclined to provide socially desirable responses rather than expressing their genuine beliefs and intentions. To mitigate this limitation, we employed a scenario-based method. As per Harrington (1996), scenarios depict the behavior of others in hypothetical situations, enabling respondents to express their true intentions without fear of judgment.

Additionally, it's important to acknowledge that the results of this study may not be universally applicable. Organizational culture has been found to exert a significant influence in information security studies. Therefore, the findings of this research may have limited generalizability beyond the context of Ethiopia. Despite these acknowledged limitations, this study has made a valuable contribution by shedding light on employees' compliance with their organizational information security policies and the impact of organizational culture on employees' compliance with information security policies. In doing so, it has advanced the body of knowledge in the field of information security, successfully achieving its research objectives.

6.5 Conclusion

This study makes it abundantly clear that protecting information security remains a moving target for the majority of organizations, despite the fact that there are a number of information security standards in place all over the world. In order to gain a deeper understanding of the issue of compliance, scholars in the field of information security have undertaken various investigations employing different theoretical frameworks, such as RCT, GDT, and protection motivation theory. Based on their respective findings, these researchers have identified factors that potentially exert a substantial impact on enhancing employees' behavior with regard to information security.

The majority of these attempts primarily concentrate on the western context, and a prevailing assumption underlying these studies is that the factors found effective in one country will similarly produce positive outcomes in another country. Contrary to this claim, a limited number

of studies have examined the influence of country-specific factors, such as organizational culture, on the outcomes of these investigations. Consequently, there is a growing demand for researchers globally to undertake investigations into the influence of organizational culture on employees' information security behavior. Therefore, our study can be regarded as an endeavor to address this urgent and crucial demand for research.

This study aimed to empirically examine the influence of constructs from rational choice theory, specifically perceived benefits, formal sanction, informal sanction, moral beliefs, and shame, on employees' intention to comply with their organization's information security policy. Furthermore, the study has conducted empirical testing on the moderating impact of various dimensions of organizational culture, specifically cooperativeness, effectiveness, consistency, and innovativeness, on the relationship between constructs of RCT and employees' intention to comply with their organization's information security policy. The empirical model proposed in this study is substantiated by the data that has been collected. In this regard, significant empirical evidence has been obtained regarding the factors that impede and facilitate employees' adherence to their organization's information security policy.

Moreover, the findings also show strong evidence on the influence of contextual factors, such as organizational culture, on employees' information security behavior, and consequently, they it highlight the importance of taking some level of precaution when organizations introduce new policies or standards that are copied from abroad. Information security policy makers and information security managers in Ethiopia, particularly at INSA, can learn how important it will be to modify or adapt their information security policy, which was copied from ISO 27002, based on the findings of this study. In addition to the practical implications of our findings, we also highlighted the contribution of our study to research and theory. Based on the limitations of the study, we also recommend opportunities for future researchers in the area of information security to further enrich the existing knowledge around factors affecting employees' information security behavior.

In the initial chapter of the dissertation, a comprehensive overview was provided, encompassing key elements such as the identification and examination of significant subjects, including the

research gap, research questions, hypotheses, and research objectives. Furthermore, we provided an overview of the research methodology employed and the literature that will be examined. In the second chapter, a comprehensive literature review was conducted to examine the key concepts relevant to the study.

Additionally, the hypotheses were supported by a thorough review of the existing literature. The third chapter of the dissertation extensively examines the research methodology, providing a comprehensive analysis of the rationale underlying each methodological decision. Furthermore, supplementary data preprocessing tasks were undertaken. In the fourth chapter, a series of validity and reliability tests were performed, which were subsequently followed by an empirical examination of the research model. This examination utilized survey data that had been collected from various regions within Ethiopia. Furthermore, a comprehensive analysis of the study's findings has been conducted. In conclusion, the fifth chapter of this study provides a comprehensive discussion on the contribution, delimitations, and implications of the research.

6.6 Recommendation for Future Studies

Despite the inherent limitations, this study has yielded intriguing findings that hold significant implications for the managers of information security policies and their stakeholders. The utilization of operationalization techniques for variables and the emphasis on the human perspective in the context of information security have rendered this study valuable for subsequent research endeavors. This study initiates the intricate endeavor of comprehending the interplay between information security and organizational culture within Ethiopian organizations. Additional steps are required in order to acquire more profound insights. This section outlines potential avenues for future research.

In this research, a survey was used to investigate the moderating influence of organizational culture on rational choice theory constructs and employees' intentions to comply with their organizational information security policy. Although this study answers the research questions stated above, there are also other issues that need further investigation by future researchers in the field.

To begin with, researchers can replicate this study in other countries using similar organizational cultures measuring methods to test its generalizability. According to the literature, information security studies use Hofstede's (2001) cultural values without measuring culture at the individual level, resulting in unsatisfactory findings on organizational culture dimensions across countries with similar cultures. Thus, we recommend future researchers conduct similar studies in developing countries to see if the findings are generalizable to at least developing countries with similar measuring methods.

Additionally, it is suggested that future researchers undertake comparable investigations employing alternative organizational cultural models, such as Schein's organizational culture model, Denison's organizational culture model, Deal and Kennedy's culture types, and O'Reilly and Chatman's organizational culture profile, as we used Cameron and Quinn's competing values framework (CVF) in this study. Repeating this study will help mature knowledge of information security policy and organizational culture in developing countries, which is a new and sensitive area of research.

Furthermore, our research model is designed to prioritize model simplicity and theoretical clarity. As a result, we have chosen to concentrate on examining the moderating impact of consistency culture on moral beliefs and compliance intention, the moderating impact of effectiveness culture on perceived benefits and compliance intention, and the moderating impact of consistency culture on formal sanctions and compliance intention, among other hypotheses outlined in our study. Nevertheless, it is crucial to acknowledge that additional research is required to investigate the moderating impact of shame and perceived benefit on consistency culture, the moderating impact of informal sanction, formal sanction, perceived benefit, and moral belief on cooperativeness culture, and the moderating impact of shame, informal sanction, formal sanction, and moral belief on effectiveness culture.

In addition, even though the theory of reasoned action states that behavioral intention predicts actual behavior (Ajzen, 1991), future studies could be conducted by using the actual compliance behavior as the dependent variable. In this regards, the result obtained from reported compliance can be compared against the result obtained from monitoring employees in their workplace. Even

though it is very difficult to objectively measure the actual compliance behavior of employees, there exists some mechanism like examining the activity log of employees on their computer or monitoring employee's computer at the end of their work hour to confirm if they obey some of the organizational security policies for example locking their computer.

In conclusion, a quantitative research method was utilized for this study. Going forward, we recommend that researchers supplement the survey method with additional interviews in order to further explain and triangulate the findings of their studies.

7. REFERENCCES

Abdul Talib, Y. and Dhillon, G. (2015). Employee ISP compliance intentions: an empirical test of empowerment.

Abebe, G. and Lessa, L. (2020). *Human factors influence in information systems security: towards a conceptual framework.* Paper presented at the Proceedings of the 2nd African International Conference on Industrial Engineering and Operations Management Harare (IEOM).

Abraham, S. (2011). Information security behavior: factors and research directions.

Adane, K. (2020). The current status of cyber security in Ethiopia. *IUP Journal of Information Technology, 16*(3), 7-19.

Akanle, O., et al. (2017). Theoretical and methodological perspectives in sociological research. *Research methods in social & management sciences*, 81-108.

Al-Mukahal, H. M. and Alshare, K. (2015). An examination of factors that influence the number of information security policy violations in Qatari organizations. *Information & Computer Security*, *23*(1), 102-118.

Alalwan, J. A. (2018). *Fear of cybercrime and the compliance with information security policies: A theoretical study.* Paper presented at the Proceedings of the 9th International Conference on E-Education, E-Business, E-Management and E-Learning.

Alharbi, S. H. and Abedelrahim, S. S. (2018). Organizational culture assessment using the competing values framework (CVF) in public universities in Saudi Arabia: A case study of Tabuk university. *International journal of business & management, 6*(2), 1-16.

Ali, R. F. and Dominic, P. (2024). Investigation of information security policy violations among oil and gas employees: A security-related stress and avoidance coping perspective. *Journal of Information Science, 50*(1), 254-272.

Aliyu, A. A., et al. (2015). *Ontology, epistemology and axiology in quantitative and qualitative research: Elucidation of the research philophical misconception.* Paper presented at the Proceedings of the Academic Conference: Mediterranean Publications & Research International on New Direction and Uncommon.

Alsolami, F. J. (2015). *Toward secure sensitive data in the cloud*: University of Colorado Colorado Springs.

Amankwa, E., et al. (2018). Establishing information security policy compliance culture in organizations. *Information & Computer Security*.

Ameri, H. (2023). Exploring information security culture within Swedish municipalities: A qualitative study. In.

Anderson, J. C. and Gerbing, D. W. (1984). The effect of sampling error on convergence, improper solutions, and goodness-of-fit indices for maximum likelihood confirmatory factor analysis. *Psychometrika, 49*, 155-173.

Andreev, P., et al. (2009). Validating formative partial least squares (PLS) models: methodological review and empirical illustration.

Antoniou, G. S. (2015). *Designing an effective information security policy for exceptional situations in an organization: An experimental study.* Nova Southeastern University,

Arage, T., et al. (2015). Influence of national culture on employees' compliance with information systems security (ISS) policies: towards ISS culture in Ethiopian companies.

Arnott, D. and Gao, S. (2022). Behavioral economics in information systems research: Critical analysis and research strategies. *Journal of Information Technology, 37*(1), 80-117.

Aurigemma, S. and Mattson, T. (2017a). Deterrence and punishment experience impacts on ISP compliance attitudes. *Information & Computer Security, 25*(4), 421-436.

Aurigemma, S. and Mattson, T. (2017b). Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. *Computers & Security, 66*, 218-234.

Barlow, J. B., et al. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security, 39*, 145-159.

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. *ACM Computing Surveys (CSUR), 25*(4), 375-414.

Becker, G. S. (1968). Crime and Punishment: An Economic Approach. *The Journal of Political Economy, 76(1830482): 169–217*.

Bhattacherjee, A. (2012). *Social science research: Principles, methods, and practices*: University of South Florida.

Bhatti, B. M., et al. (2021). *Factors Impacting Information Security Risk Management in IT Outsourcing: An Agency Theory Perspective.* Paper presented at the PACIS.

Boss, S. R., et al. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS quarterly, 39*(4), 837-864.

Bouchrika, I. (2021). What is empirical research? Definition, types & samples. *Research. com, 8*.

Brazevich, D. S., et al. (2020). Analysis of the Problems of Ensuring Information Security in the Terms of the Contemporary Society. *Open Journal of Social Sciences, 8*(2), 231-241.

Browne, S. (2018). The Insider Threat. *Comparing malicious and non-malicious information security behaviours using a rational choice model*.

Bulgurcu, B., et al. (2009). *Effects of Individual and Organization Based Beliefs and the Moderating Role of Work Experience on Insiders' Good Security Behaviors*. Paper presented at the 2009 International Conference on Computational Science and Engineering.

Bulgurcu, B., et al. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 523-548.

Burrell, G., et al. (1979). Assumptions about the nature of social science. *Sociological paradigms and organisational analysis, 248*(1), 1-9.

Butler, K. J. and Brown, I. (2023). COVID-19 pandemic-induced organisational cultural shifts and employee information security compliance behaviour: a South African case study. *Information & Computer Security, 31*(2), 221-243.

Cameron, K. (2009). An introduction to the competing values framework. *Organizational culture white paper. Haworth*.

Cameron, K. and Sine, W. (1999). A framework for organizational quality culture. *Quality Management Journal, 6*(4), 7-25.

Cameron, K. S. (1985). Cultural Congruence, Strength, and Type: Relationships to Effectiveness. ASHE 1985 Annual Meeting Paper.

Cardoso, A. C. H. and Ramos, I. (2012). *Looking at the past to enrich the future: A reflection on Klein and Myers' quality criteria for interpretive research*.

Cavana, R., et al. (2001). *Applied business research: Qualitative and quantitative methods*: John Wiley & Sons.

Chaâri, R., et al. (2016). Cyber-physical systems clouds: A survey. *Computer Networks, 108*, 260-278.

Chatman, J. A. and Jehn, K. A. (1994). Assessing the relationship between industry characteristics and organizational culture: how different can you be? *Academy of management journal, 37*(3), 522-553.

Chen, X., et al. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management, 55*(8), 1049-1060.

Cheng, L., et al. (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.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern methods for business research, 295*(2), 295-336.

Choi, M. and Song, J. (2018). Social control through deterrence on the compliance with information security policy. *Soft Computing, 22*(20), 6765-6772.

Chua, W. F. (1986). Radical developments in accounting thought. *Accounting review*, 601-632.

Clark, T., et al. (2021). *Bryman's social research methods*: Oxford university press.

Clemons, E. K., et al. (2017). Understanding the information-based transformation of strategy and society. *Journal of Management Information Systems, 34*(2), 425-456.

Cohen, J. (1998). Statistical power analysis for the behavioural sciences, xxi. *Hillsdale, NJ: L Erlbaum Associates*.

Cohen, J. (2013). *Statistical power analysis for the behavioral sciences*: Routledge.

Collin, J. and Hussy, R. (2009). Business Research, A Practical Guide for Undergraduate and Postgraduate Student. *Hampshire: Palgrave Macmillan*.

Cram, W. A., et al. (2019). 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., et al. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems, 26*, 605-641.

Creswell, J. W. and Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*: Sage publications.

Crossler, R. E., et al. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101. doi:10.1016/j.cose.2012.09.010

Cyprian Maphanga, G. and Jokonya, O. (2017). THE RISK OF USERS'NEGATIVE BEHAVIOURS INFLUENCE ON INFORMATION SECURITY COMPLIANCE POLICY IN ORGANIZATIONS. *Risk Governance & Control: Financial Markets & Institutions, 7*(4).

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

D'Arcy, J., et al. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information systems research, 20*(1), 79-98.

D'Arcy, J. and Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal, 29*(1), 43-69.

D'Arcy, J. and Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of business ethics, 89*, 59-71.

Damamisau, M. S. S., BASHIR ALI, et al. (2020). UNDERSTANDING PHILOSOPHICAL ASSUMPTIONS IN SOCIAL SCIENCE RESEARCH: A CONTRIBUTORY NOTE. *LAPAI INTERNATIONAL JOURNAL ADMINISTRATION, 3*(2), 156-170.

de Boer, H. and Goedegebuure, L. (2014). Exploring organisational culture in Saudi Arabian higher education: Interim report.

Denison, D. R., et al. (2004). Corporate culture and organizational effectiveness: is Asia different from the rest of the world? *Organizational dynamics, 33*(1), 98-109.

Desisa, A. and Beshah, T. (2014). Internet banking security framework: the case of ethiopian banking industry. *HiLCoE J Comput Sci Tech, 2*(2).

Detert, J. R., et al. (2000). A framework for linking culture and improvement initiatives in organizations. *Academy of Management Review, 25*(4), 850-863.

Dhillon, G. and Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127-153.

Di Stefano, G., et al. (2019). The effect of organizational culture on deviant behaviors in the workplace. *The International Journal of Human Resource Management, 30*(17), 2482-2503.

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

Dols, T. and Silvius, A. (2010). Exploring the influence of national cultures on non-compliance behavior. *Communications of the IIMA, 10*(3), 2.

Doupnik, T. S. and Tsakumis, G. T. (2004). A critical review of tests of Gray's theory of cultural relevance and suggestions for future research. *Journal of accounting literature, 23*, 1.

Dzazali, S., et al. (2009). Employing the social-technical perspective in identifying security management systems in organisations. *International Journal of Business Information Systems, 4*(4), 419-439.

Ejerssa, N. (2018). *Assessment of information security maturity level on Ethiopian public universities.* MSc. Thesis, Addis Ababa University (Unpublished),

Ejigu, K., et al. (2023). The moderating impact of organizational culture on information security compliance. *SINET: Ethiopian Journal of Science, 46*(3), 250-270.

Elis, L. A. and Simpson, S. S. (1995). Informal sanction threats and corporate crime: Additive versus multiplicative models. *Journal of Research in Crime and Delinquency, 32*(4), 399-424.

Ernest Chang, S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438-458. doi:10.1108/02635570710734316

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

Eskelinen, E. (2019). *Factors affecting information security behavior of employees: a case study*.

Faber, J. and Fonseca, L. M. (2014). How sample size influences research outcomes. *Dental press journal of orthodontics, 19*, 27-29.

Farayola, O. A., et al. (2024). Data privacy and security in IT: a review of techniques and challenges. *Computer Science & IT Research Journal, 5*(3), 606-615.

Flowerday, S. V. and Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security, 61*, 169-183.

Foley, S. N. and Rooney, V. M. (2019). *Social Constructionism in Security Protocols: A Position on Human Experience, Psychology and Security*. Paper presented at the Cambridge International Workshop on Security Protocols.

Fong, L. H. N. and Law, R. (2013). Hair, J. F. Jr., Hult, G. T. M., Ringle, C. M., Sarstedt, M. (2014). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). Sage Publications. ISBN: 978-1-4522-1744-4. 307 pp. *European Journal of Tourism Research*.

Garza, V. and Guo, X. (2015). Securing BYOD: A study of framing and neutralization effects on mobile device security policy compliance.

Gefen, D. and Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the association for information systems, 16*(1), 5.

Gefen, D., et al. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the association for information systems, 4*(1), 7.

George, D. and Mallery, P. (2019). *IBM SPSS statistics 26 step by step: A simple guide and reference*: Routledge.

Getaneh, T. (2018). Cyber Security Practices and Challenges at Selected Critical Infrastructures in Ethiopia: Towards Tailoring Cyber Security Framework. In: Addis Ababa University.

Ghasemy, M., et al. (2020). This fast car can move faster: A review of PLS-SEM application in higher education research. *Higher education, 80*(6), 1121-1152.

Gichuru, M. J. (2017). The interpretive research paradigm: A critical review of is research methodologies. *International Journal of Innovative Research and Advanced Studies (IJIRAS), 4*(2), 1-5.

Gordon, G. G. and DiTomaso, N. (1992). Predicting corporate performance from organizational culture. *Journal of management studies, 29*(6), 783-798.

Grasmick, H. G. and Bursik Jr, R. J. (1990). Conscience, significant others, and rational choice: Extending the deterrence model. *Law and Society Review*, 837-861.

Hair, J. F., et al. (2021). Executing and interpreting applications of PLS-SEM: Updates for family business researchers. *Journal of family business strategy, 12*(3), 100392.

Hair, J. F., et al. (2013). Partial least squares structural equation modeling: Rigorous applications, better results and higher acceptance. *Long range planning, 46*(1-2), 1-12.

Hair Jr, J. F., et al. (2020). Assessing measurement model quality in PLS-SEM using confirmatory composite analysis. *Journal of business research, 109*, 101-110.

Hair Jr, J. F., et al. (2021). *A primer on partial least squares structural equation modeling (PLS-SEM)*: Sage publications.

Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2014). A primier on partial least squares structural equation modeling (PLS-SEM). Sage Publications, Incorporated.

Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017). A primer on partial least squares structural equation modeling (PLS-SEM) (2nd Editio). *Thousand Oaks, CA.: Sage publications*.

Hair Jr, J. F., et al. (2017). PLS-SEM or CB-SEM: updated guidelines on which method to use. *International Journal of Multivariate Data Analysis, 1*(2), 107-123.

Han, J., et al. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security, 66*, 52-65.

Hanafiah, M. H. (2020). Formative vs. reflective measurement model: Guidelines for structural equation modeling research. *International Journal of Analysis and Applications, 18*(5), 876-889.

Harvey, A., et al. (2012). The future of technologies for personalised medicine. *New biotechnology, 29*(6), 625-633.

Henseler, J., et al. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the academy of marketing science, 43*, 115-135.

Herath, T. and Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*, 106-125.

Hina, S. and Dominic, D. D. (2016). *Information security policies: Investigation of compliance in universities.* Paper presented at the 2016 3rd International Conference on Computer and Information Sciences (ICCOINS).

Hofstede, G. (1984). *Culture's consequences: International differences in work-related values* (Vol. 5): sage.

Hofstede, G. (2011). National cultures, organizational cultures, and the role of management. *Values and Ethics for the 21st Century*, 385-403.

Hofstede, G., et al. (1990). Measuring organizational cultures: A qualitative and quantitative study across twenty cases. *Administrative science quarterly*, 286-316.

Hooper, V. and Blunt, C. (2020). Factors influencing the information security behaviour of IT employees. *Behaviour & Information Technology, 39*(8), 862-874.

Howard, L. W. (1998). Validating the competing values model as a representation of organizational cultures. *The international journal of organizational analysis, 6*(3), 231-250.

Hu, Q., et al. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decis. Sci., 43*, 615-660.

Hu, Q., et al. (2015). The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems, 31*(4), 6-48.

Hu, Q., et al. (2010). Why individuals commit computer offences in organizations: Investigating the roles of rational choice, self-control, and deterrence.

Hu, Q., et al. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54*(6), 54-60.

Huang, H.-W., et al. (2016). *Willingness and Ability to Perform Information Security Compliance Behavior: Psychological Ownership and Self-Efficacy Perspective.* Paper presented at the PACIS.

Hubona, G. S. (2009). Structural equation modeling (SEM) using SmartPLS software: analyzing path models using partial least squares (PLS) based SEM.

Humaidi, N. and Balakrishnan, V. (2015). The moderating effect of working experience on health information system security policies compliance behaviour. *Malaysian Journal of Computer Science, 28*(2), 70-92.

Hwang, I., et al. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review, 41*(1), 2-18.

Idahosa, M. D. (2020). *Strategies for implementing successful IT security systems in small businesses.* Walden University,

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

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

Ifinedo, P. (2016). Critical times for organizations: what should be done to curb workers' noncompliance with IS security policy guidelines? *Information Systems Management, 33*(1), 30-41.

Interligi, L. (2010). Compliance culture: A conceptual framework. *Journal of Management & Organization, 16*(2), 235-249.

Jan, J., et al. (2022). Hofstede's cultural dimensions in technology acceptance models: a meta-analysis. *Universal Access in the Information Society*, 1-25.

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

Johnston, A. C., et al. (2015). An enhanced fear appeal rhetorical framework. *MIS quarterly, 39*(1), 113-134.

Kalof, L. and Dan, A. (2008). *Essentials of social research*: McGraw-Hill Education (UK).

Kam, H.-J. and Katerattanakul, P. (2014). Information security in higher education: A neo-institutional perspective. *Journal of information privacy and security, 10*(1), 28-43.

Karlsson, M., et al. (2022). The effect of perceived organizational culture on employees' information security compliance. *Information & Computer Security, 30*(3), 382-401.

Kennedy, A. A. (1982). *Corporate cultures: The rites and rituals of corporate life*: Reading, Mass.; Don Mills, Ontario: Addison-Wesley Publishing Company.

Khatib, R. and Barki, H. (2022). How different rewards tend to influence employee non-compliance with information security policies. *Information & Computer Security, 30*(1), 97-116.

Kim, J.-k. and Oh, D.-W. (2018). A Study on Security Policy Violations of Organization Members. *Informatization Policy, 25*(3), 95-115.

King, F. and Paul, S. (2024). Neutralization Tendencies in Information Systems Security Violation.

Kolokotronis, N., et al. (2002). An integrated approach for securing electronic transactions over the web. *Benchmarking: An International Journal, 9*(2), 166-181.

Kraemer, S. and Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics, 38*(2), 143-154.

Kuppusamy, P., et al. (2022). Information security policy compliance behavior models, theories, and influencing factors: A systematic literature review. *Journal of Theoretical and Applied Information Technology, 100*(5), 1536-1557.

Kwan, P. and Walker, A. (2004). Validating the competing values model as a representation of organizational culture through inter-institutional comparisons. *Organizational Analysis, 12*(1), 21-37.

Latan, H., et al. (2017). Partial least squares path modeling. *Partial least squares path modeling: basic concepts, methodological issues and applications*.

Leidner, D. E. and Kayworth, T. (2006). A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS quarterly*, 357-399.

Leidner, D. E. and Kayworth, T. R. (2014). Knowledge management and organizational culture. In *Knowledge Management* (pp. 40-60): Routledge.

Li, H., et al. (2021). Understanding information security policy violation from a situational action perspective. *Journal of the Association for Information Systems, 22*(3), 5.

Li, H., et al. (2018). Self-control, organizational context, and rational choice in Internet abuses at work. *Information & Management, 55*(3), 358-367.

Li, H., et al. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*(4), 635-645.

Liang, H., et al. (2013). Ensuring employees' IT compliance: carrot or stick? *Information systems research, 24*(2), 279-294.

Lickel, B., et al. (2014). Shame and the motivation to change the self. *Emotion, 14*(6), 1049.

Lim, J. S., et al. (2009). Exploring the relationship between organizational culture and information security culture.

Liu, C., et al. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management, 54*, 102152.

Malatji, M., et al. (2020). Validation of a socio-technical management process for optimising cybersecurity practices. *Computers & Security, 95*, 101846.

McCumber, J. (2011). The failure of rational choice philosophy. *The New York Times, 19*.

McFadzean, E., et al. (2006). Anchoring information security governance research: sociological groundings and future directions. *Journal of Information System Security, 2*(3), 3-48.

Meng, F., et al. (2016). The influence of organizational culture on talent management: A case study of a real estate company. *Journal of Chinese Human Resource Management, 7*(2), 129-146.

Merhi, M. and Ahluwalia, P. (2015). Top management can lower resistance toward information security compliance.

Mohajan, H. K. (2020). Quantitative research: A successful investigation in natural and social sciences. *Journal of Economic Development, Environment and People, 9*(4), 50-79.

Moody, G. D., et al. (2018). Toward a unified model of information security policy compliance. *MIS quarterly, 42*(1).

Mosqueda, S. (2023). *Cost Of Insider Risks Global Report*. Retrieved from

Myers, M. D. and Klein, H. K. (2011). A set of principles for conducting critical research in information systems. *MIS quarterly*, 17-36.

Myyry, L., et al. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems, 18*(2), 126-139.

Nagin, D. S. and Paternoster, R. (1993). Enduring individual differences and rational choice theories of crime. *Law and Society Review*, 467-496.

Nelson, R. E. and Gopalan, S. (2003). Do organizational cultures replicate national cultures? Isomorphism, rejection and reciprocal opposition in the corporate values of three countries. *Organization studies, 24*(7), 1115-1151.

O'Reilly III, C. A., et al. (1991). People and organizational culture: A profile comparison approach to assessing person-organization fit. *Academy of management journal, 34*(3), 487-516.

Opoku, A., et al. (2016). Choosing an appropriate research methodology and method. In *Research methodology in the built environment* (pp. 32-49): Routledge.

Pahnila, S., et al. (2007). Which factors explain employees' adherence to information security policies? An empirical study.

Park, Y. S., et al. (2020). The positivism paradigm of research. *Academic medicine, 95*(5), 690-694.

Paternoster, R. and Pogarsky, G. (2009). Rational choice, agency and thoughtfully reflective decision making: The short and long-term consequences of making good choices. *Journal of Quantitative Criminology, 25*, 103-127.

Paternoster, R. and Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law and Society Review*, 549-583.

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*: CRC press.

Pfister, J. A. (2009). *Managing organizational culture for effective internal control: From practice to theory*: Springer Science & Business Media.

Pieters, W. (2017). Beyond individual-centric privacy: Information technology in social systems. *The Information Society, 33*(5), 271-281.

Plog, F., et al. (1976). Anthropology: Decisions, Adaptation, andEvolution. In: Knopf, New York. PlogAnthropology: Decisions, Adaptation, and Evolution1976.

Podsakoff, P. M., et al. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *J Appl Psychol*, *88*(5), 879-903. doi:10.1037/0021-9010.88.5.879

Pogarsky, G. (2009). Deterrence and decision making: Research questions and theoretical refinements. *Handbook on crime and deviance*, 241-258.

Pogarsky, G. and Piquero, A. R. (2004). Studying the reach of deterrence: Can deterrence theory help explain police misconduct? *Journal of criminal justice, 32*(4), 371-386.

Pratt, T. C., et al. (2006). The empirical status of deterrence theory: A meta-analysis.

Puhakainen, P. (2006). A design theory for information security awareness.

Puhakainen, P. and Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS quarterly*, 757-778.

Quinn, R. E. (2011). *Diagnosing and changing organizational culture: Based on the competing values framework*: Jossey-Bass.

Quinn, R. E. and Spreitzer, G. M. (1991). *The psychometrics of the competing values culture instrument and an analysis of the impact of organizational culture on quality of life*: Emerald.

Rahi, S. (2017). Research design and methods: A systematic review of research paradigms, sampling issues and instruments development. *International Journal of Economics & Management Sciences, 6*(2), 1-5.

Raja, S. (2023). *Insider Threat Report Finds*. Retrieved from

Ralston, D. A., et al. (2006). Today's state-owned enterprises of China: are they dying dinosaurs or dynamic dynamos? *Strategic management journal, 27*(9), 825-843.

Rashid, A., et al. (2021). A Quantitative Perspective of Systematic Research: Easy and Step-by-Step Initial Guidelines. *Turkish Online Journal of Qualitative Inquiry, 12*(9).

Ringle, C. M., et al. (2012). A critical look at the use of PLS-SEM in MIS quarterly. MIS Q. Manag. *Inf. Syst, 36*(1).

Robinson, W. S. (2009). Ecological correlations and the behavior of individuals. *International journal of epidemiology, 38*(2), 337-341.

Sarkar, S., et al. (2020). The influence of professional subculture on information security policy violations: A field study in a healthcare context. *Information systems research, 31*(4), 1240-1259.

Sarstedt, M., et al. (2019). How to specify, estimate, and validate higher-order constructs in PLS-SEM. *Australasian marketing journal, 27*(3), 197-211.

Schein, E. H. (1983). Organizational culture: A dynamic model.

Schein, E. H. (2010). *Organizational culture and leadership* (Vol. 2): John Wiley & Sons.

Schlienger, T. and Teufel, S. (2002). Information security culture: The socio-cultural dimension in information security management. *Security in the information society: Visions and perspectives*, 191-201.

Securonix. (2024). Securonix | 2024 Insider Threat Report.

Sharma, S. and Warkentin, M. (2019). Do I really belong?: Impact of employment status on information security policy compliance. *Computers & Security, 87*, 101397.

Shimels, T. and Lessa, L. (2023). Maturity of information systems' security in Ethiopian banks: case of selected private banks. *International Journal of Industrial Engineering and Operations Management*(ahead-of-print).

Silic, M., et al. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Information & Management, 54*(8), 1023-1037.

Siponen, M. (2002). Towards maturity of information security maturity criteria: six lessons learned from software maturity criteria. *Information Management & Computer Security, 10*(5), 210-224.

Siponen, M., et al. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.

Siponen, M., et al. (2007). *Employees' adherence to information security policies: an empirical study.* Paper presented at the New Approaches for Security, Privacy and Trust in Complex Environments: Proceedings of the IFIP TC-11 22 nd International Information Security Conference (SEC 2007), 14–16 May 2007, Sandton, South Africa 22.

Siponen, M., et al. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64-71.

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

Siponen, M. and Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. *European Journal of Information Systems, 23*(3), 289-305.

Siponen, M., et al. (2012). New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs. *Information & Management, 49*(7-8), 334-341.

Siponen, M. T. (2001). Five dimensions of information security awareness. *SIGCAS Comput. Soc., 31*(2), 24-29.

Solomon, G. and 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.

Sommestad, T. and Hallberg, J. (2013). *A review of the theory of planned behaviour in the context of information security policy compliance.* Paper presented at the Security and Privacy Protection in Information Processing Systems: 28th IFIP TC 11 International Conference, SEC 2013, Auckland, New Zealand, July 8-10, 2013. Proceedings 28.

Sommestad, T., et al. (2014). Variables influencing information security policy compliance. *Information Management & Computer Security, 22*(1), 42-75. doi:10.1108/imcs-08-2012-0045

Sommestad, T., et al. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security, 23*(2), 200-217.

Soomro, Z. A., et al. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215-225.

Srite, M. and Karahanna, E. (2006). The role of espoused national cultural values in technology acceptance. *MIS quarterly*, 679-704.

Stanton, J. M., et al. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.

Straub, D., et al. (2004). Validation guidelines for IS positivist research. *Communications of the association for information systems, 13*(1), 24.

Straub, D., et al. (2002). Toward a theory-based measurement of culture. *Journal of Global Information Management (JGIM), 10*(1), 13-23.

Straub, D. W. and Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS quarterly*, 441-469.

Straub Jr, D. W. and Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS quarterly*, 45-60.

Streukens, S. and Leroi-Werelds, S. (2016). Bootstrapping and PLS-SEM: A step-by-step guide to get more out of your bootstrap results. *European management journal, 34*(6), 618-632.

Susanto, H. and Almunawar, M. N. (2018). *Information security management systems: a novel framework and software as a tool for compliance with information security standard*: Apple Academic Press.

Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in science education, 48*, 1273-1296.

Tadesse, K., et al. (2021). Influence of Organizational Culture on Employees' Compliance with Information Security Policy: Ethiopian and Finland Companies.

Takemura, T. (2014). Empirical analysis of intentional security policy violation in the workplace. *佐賀大学経済論集/**佐賀大学経済学会***, *46*(6), 21-40.

Talib, Y. Y. A. (2015). *Intrinsic motivation and information systems security policy compliance in organizations*: Virginia Commonwealth University.

Tang, M. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management, 17*, 179-186.

Tang, M., et al. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management, 17*, 179-186.

Tarafdar, M., et al. (2014). The dark side of information technology. *MIT Sloan Management Review*.

Team, S. C. I. (2022). *African Cyberthreat Assessment Report*. Retrieved from

Tenenhaus, M., et al. (2005). PLS path modeling. *Computational statistics & data analysis*, *48*(1), 159-205.

Theis, M., et al. (2019). Common sense guide to mitigating insider threats.

Thomson, K.-L. and Von Solms, R. (2005). Information security obedience: a definition. *Computers & Security, 24*(1), 69-75.

Thomson, K.-L., et al. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security, 2006*(10), 7-11.

Tilahun, A. and Tibebe, T. (2017). INFLUENCE OF NATIONAL CULTURE ON EMPLOYEES'INTENTION TO VIOLATE INFORMATION SYSTEMS SECURITY POLICIES: A NATIONAL CULTURE AND RATIONAL CHOICE THEORY PERSPECTIVE.

Togia, A. and Malliari, A. (2017). Research methods in library and information science. *Qualitative versus quantitative research, 52*.

Trang, S. and Brendel, B. (2019). A meta-analysis of deterrence theory in information security policy compliance research. *Information Systems Frontiers, 21*, 1265-1284.

Triandis, H. C. and Suh, E. M. (2002). Cultural influences on personality. *Annual review of psychology, 53*(1), 133-160.

Trim, P. R. and Lee, Y.-I. (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. *Industrial Marketing Management, 83*, 224-238.

Tsai, Y. (2011). Relationship between organizational culture, leadership behavior and job satisfaction. *BMC health services research, 11*, 1-9.

Tsakumis, G. T., et al. (2007). The relation between national cultural dimensions and tax evasion. *Journal of international accounting, auditing and taxation, 16*(2), 131-147.

Tsohou, A. and Holtkamp, P. (2018). Are users competent to comply with information security policies? An analysis of professional competence models. *Information Technology & People, 31*(5), 1047-1068.

Tsui, A. S., et al. (2006). Unpacking the relationship between CEO leadership behavior and organizational culture. *The Leadership Quarterly, 17*(2), 113-137.

Tyler, T. R. and Blader, S. L. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of management journal, 48*(6), 1143-1158.

Ugrin, J. C. and Pearson, J. M. (2010). Understanding the effect of deterrence mechanisms on cyberloafing: Exploring a general deterrence model with a social perspective.

Urbach, N. and Ahlemann, F. (2010). Structural equation modeling in information systems research using partial least squares. *Journal of Information Technology Theory and Application (JITTA), 11*(2), 2.

Van Muijen, J. J. (1999). Organizational culture: The focus questionnaire. *European Journal of work and organizational psychology, 8*(4), 551-568.

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

Vance, A., et al. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49*(3-4), 190-198. doi:10.1016/j.im.2012.04.002

Vance, A. and Siponen, M. T. (2012). IS Security Policy Violations. *Journal of Organizational and End User Computing, 24*(1), 21-41. doi:10.4018/joeuc.2012010102

Vance, A., et al. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. *Information & Management, 57*(4), 103212.

Von Solms, B. (2006). Information security–the fourth wave. *Computers & Security, 25*(3), 165-168.

Von Solms, B. and Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security, 23*(5), 371-376.

Vroom, C. and von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198. doi:10.1016/j.cose.2004.01.012

Waly, N. S. (2013). *Organisational information security management: The impact of training and awareness. Evaluating the socio-technical impact on organisational information security policy management.* University of Bradford,

Warkentin, M., et al. (2012). Impact of protection motivation and deterrence on is security policy compliance: a multi-cultural view.

Waziri, B. Z. and Kyari, A. K. (2023). Adopting A Research Methodology in Management Sciences: An Appropriate Guide for Postgraduate Researchers. *International Journal of Accounting, Finance and Administrative Research, 1*(1), 196-206.

Wenzel, M. (2004). The social side of sanctions: Personal and social norms as moderators of deterrence. *Law and human behavior, 28,* 547-567.

Whipple, D. W. (2015). *The effects of organizational culture traits on information security principles for organizations located in the United States: An exploratory quantitative study.*

Willcocks, L. and Margetts, H. (1994). Risk assessment and information systems. *European Journal of Information Systems, 3*(2), 127-138.

Willison, R. and Backhouse, J. (2006). Opportunities for computer crime: considering systems risk from a criminological perspective. *European Journal of Information Systems, 15*(4), 403-414.

Willison, R. and Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS quarterly*, 1-20.

Woretaw, A. and Lessa, L. (2012). *Information security culture in the banking sector in Ethiopia.* Paper presented at the 5th ICT 2012 Ethiopia Conference.

Yazdanmehr, A., et al. (2024). The role of ethical climates in employee information security policy violations. *Decision Support Systems, 177*, 114086.

Yazdanmehr, A. and Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems, 92*, 36-46.

Yazdanmehr, A. and Wang, J. (2023). Can peers help reduce violations of information security policies? The role of peer monitoring. *European Journal of Information Systems, 32*(3), 508-528.

Yazdanmehr, A., et al. (2020). Peers matter: The moderating role of social influence on information security policy compliance. *Information Systems Journal, 30*(5), 791-844.

Yohannes, T., et al. (2019). Information security incident response management in an Ethiopian bank: A gap analysis.

Yu, T. and Wu, N. (2009). A review of study on the competing values framework. *International journal of business and management, 4*(7), 37-42.

8. APPENDIX I: The Research Instruments

Demographic Information:

1. Age: _____
2. Gender: ___Male ____ Female
3. Education: ___High school graduate ___Vocational/some college ___Bachelors __ Masters __Doctoral
4. How realistic is the given scenario?

___Non-realistic _____Somewhat realistic ____Realistic

5. Scenario type you received to respond

___Type 1 _____Type 2 ____Type 3

6. Years of computer usage:

___ ≥ 10years ___ ≥ 5 years ___ ≥ 2 years ___< 2 year 50.

7. What is your current employment status? _____Student ____Employee _____Retired _____Other

Using the five-point scale provided below, please indicate if you agree or disagree with the following statements.

1 = Strongly Disagree, 2 = Disagree, 3= Neither, 4 = Agree, 5 = Strongly Agree

Hypothetical Scenario:

Password sharing

Casey splits her time working in the offices of two different degree programs offered at the university. In one of the offices, she is responsible for tracking the current status of research grant funding allocations for the entire department; this information is accessed using a special program that is only loaded on her office computer hard drive. Casey is aware of the university's policy that each computer workstation must be password protected and that passwords are not to be shared. However, since Casey moves between job locations regularly, she shared the password to her office computer with several coworkers so that they can get the information they need when they need it. Casey expects that sharing her password will save her coworkers a lot

of time and effort instead of waiting for her to get back to the office (Moody et al., 2018; M. Siponen and Vance, 2010).

Workstation logout

Jordan works in the front office of a popular degree program offered at the university. His duties require frequent interaction with faculty, staff, students, and outside clients both at and away from his desk. Jordan is aware of the university's policy that employees must log out of or lock their computer workstation when not using it. When Jordan knows or believes he is going to be away from his desk for an extended period of time (one hour or longer), he locks his computer. However, based upon his typical schedule of frequent departures to and from his desk, Jordan mostly keeps his user account logged-in to save him time in performing his normal duties (Moody et al., 2018; M. Siponen and Vance, 2010).

Sharing customer information

Jack is working in a position that requires access to his company customers' personal information. His company's information security policy prohibit him from giving the customer's personal information detail to anyone, except the main office. Jack is expected to send some of the customers' personal information to the main office but the internet connection in his office is too slow to send the data. Therefore, Jack believes that asking his friend to send the customer information from his office with a convenient internet connection could save a lot time and money for the company. He also know that an employee was recently reprimanded for sending the data through unauthorized person. Jack gives the data to his friend so that he will send it to the main office (Arage et al., 2015).

USB drive

Pekka is a middle level manager in a medium-sized company where he has worked for several years. Pekka is currently working on a sales report that requires the analysis of the company's customer database. This database contains customer names, phone numbers, credit card numbers, and purchase histories. Because of the sensitive nature of corporate data, the company has a strict policy prohibiting the copy of corporate data to unencrypted portable media, such as

USB drives. However, Pekka will be traveling for several days and would like to analyze the corporate database on the road. Pekka expects that copying the data to the USB drive and taking it on the road could save the company a lot of time and money. The firm is experiencing growing sales and revenues in an industry that is economically deteriorating. He also knows that an employee was recently reprimanded for copying sensitive corporate data to a USB drive. Pekka copies the corporate database to his portable USB drive and takes it off company premises (M. Siponen and Vance, 2010).

Failing to report computer virus

Gina is browsing possible questionable websites at work and the anti-virus program alerts her that a virus has been installed on her computer. Although the information security policy requires that IT support staff remove viruses, Gina decides to take care of the virus problem by herself (Vance et al., 2012).

Construct	Definition and Item Source(s)	Item code	Survey Question/Measurement Item	Section One Please provide your level of agreement or disagreement with the following statements. (Please mark only one 'X' for each line in the labeled column) Strongly Disagree=1 Disagree=2 Neutral =3 Agree=4 Strongly Agree=5	1	2	3	4	5
Cooperativeness	The organization emphasizing cooperativeness is typically a friendly place where its members share information and trust one another just like an extended family. Items adapted from Chang and Lin (2007)	COOP_1	Managers empower staff	Employees who have been given the authority, power, and means for making decisions in the interest of the organization are considered empowered employees. In this organization, managers empower their staff.					
		COOP_2	Managers treat all staff as their big family members.	In this organization, managers treat all staff as their big family members.					
		COOP_3	Employees are loyal and trust one another.	Employees are loyal and trust one another.					
		COOP_4	Your organization encourages employees to actively participate all company activities and events.	Your organization encourages employees to actively participate all company activities and events.					
		COOP_5	Employees are devoted to protect their organization.	Employees are devoted to protect their organization.					

Construct	Definition and Item Source(s)	Item code	Survey Question/Measurement Item	Section One Please provide your level of agreement or disagreement with the following statements. (Please mark only one 'X' for each line in the labeled column) Strongly Disagree=1 Disagree=2 Neutral =3 Agree=4 Strongly Agree=5	1	2	3	4	5
		COOP_6	Employees are trusted by their managers, and can participate in the decision making process.	Employees are trusted by their managers, and can participate in the decision making process.					
		COOP_7	It is very harmonious amongst employees, and your company is treated like a big family.	It is very harmonious amongst employees, and your company is treated like a big family.					
		COOP_8	Your Company pays attentions to human resource development, employees' morale, and teamwork.	Your Company pays attentions to human resource development, employees' morale, and teamwork.					
Innovativeness	The company emphasizing innovativeness supports a fully creative and dynamic environment. Additionally, organizational cultures oriented toward	INNO_1	Managers have courage to make innovation and take risk.	Managers have courage to make innovation and take risk.					
		INNO_2	Managers actively lead the staff to grow and innovate.	Managers actively lead the staff to grow and innovate.					
		INNO_3	Managers have vision and insights to create new business opportunities.	Managers have vision and insights to create new business opportunities.					

Construct	Definition and Item Source(s)	Item code	Survey Question/Measurement Item	Section One Please provide your level of agreement or disagreement with the following statements. (Please mark only one 'X' for each line in the labeled column) Strongly Disagree=1 Disagree=2 Neutral =3 Agree=4 Strongly Agree=5	1	2	3	4	5
	innovativeness recognize opportunity in change, push boundaries, and embrace creativity (Cameron, Quinn, DeGraff, & Thakor, 2014). Items adapted from Chang and Lin (2007)	INNO_4	Employees always have to face challenges and they can learn and grow from the challenges.	Employees always have to face challenges and they can learn and grow from the challenges.					
		INNO_5	Your Company pays attentions to the uniqueness of employees and encourages the innovation from employees.	Your Company pays attentions to the uniqueness of employees and encourages the innovation from employees.					
		INNO_6	Your Company is willing to take risks, and it is indeed an ambitious and energetic organization.	Your Company is willing to take risks, and it is indeed an ambitious and energetic organization.					
Consistency	The company emphasizing consistency is typically a formalized and regular organization. Consistency:	CONS_1	Managers set up clear goals and demand employees to carry out the goals strictly.	Managers set up clear goals and demand employees to carry out the goals strictly.					
		CONS_2	Your Company always has formal and strict rules for employees to follow.	Your Company always has formal and strict rules for employees to follow.					

Construct	Definition and Item Source(s)	Item code	Survey Question/Measurement Item	Section One Please provide your level of agreement or disagreement with the following statements. (Please mark only one 'X' for each line in the labeled column) Strongly Disagree=1 Disagree=2 Neutral =3 Agree=4 Strongly Agree=5	1	2	3	4	5
	refers to aspects of control and internal processes, which emphasize order, rules and regulations, uniformity, and efficiency (Chang & Lin, 2007; Quinn & Rohrbaugh, 1983). Items adapted from Chang and Lin (2007).	CONS_3	The operation of your company emphasizes stability and conservative culture. It does not allow any confusion.	The operation of your company emphasizes stability and conservative culture. It does not allow any confusion.					
		CONS_4	Your Company pays attentions to efficiency and performance for achieving the goals.	Your Company pays attentions to efficiency and performance for achieving the goals.					
		CONS_5	Your Company is stable and offers job security to employees.	Your Company is stable and offers job security to employees.					
		CONS_6	Your Company is a systematic organization where each employee has clear duty, and its operations are well defined with clear rules to follow.	Your Company is a systematic organization where each employee has clear duty, and its operations are well defined with clear rules to follow.					
	The company emphasizing effectiveness is	EFFE_1	Managers emphasize working efficiency and acts effectively.	Managers emphasize working efficiency and acts effectively.					

Construct	Definition and Item Source(s)	Item code	Survey Question/Measurement Item	Section One Please provide your level of agreement or disagreement with the following statements. (Please mark only one 'X' for each line in the labeled column) Strongly Disagree=1 Disagree=2 Neutral =3 Agree=4 Strongly Agree=5	1	2	3	4	5
Effectiveness	Primarily a result-oriented and benefit-oriented organization. The specific traits explored by this study were competitiveness, goal achievement, production, and benefit-oriented measures. Items adapted from Chang and Lin (2007).	EFFE_2	Managers pay attentions to achieve good work performance and reach the goal, regardless of personal feelings.	Managers pay attentions to achieve good work performance and reach the goal, regardless of personal feelings.					
		EFFE_3	The critical success factor of your company is its good productivity.	The critical success factor of your company is its good productivity.					
		EFFE_4	Your Company pays attentions to work efficiency. Every department and	Your Company pays attentions to work efficiency. Every department and					
		EFFE_5	Your Company pays attentions to maintaining its competition advantages.	Your Company pays attentions to maintaining its competition advantages.					
		EFFE_6	Your Company pays attentions to employees in terms of increasing their efficiency and pursuing their accomplishment.	Your Company pays attentions to employees in terms of increasing their efficiency and pursuing their accomplishment.					

Construct	Definition and Item Source(s)	Item code	Survey Question/Measurement Item	**Section One** **Please provide your level of agreement or disagreement with the following statements. (Please mark only one 'X' for each line in the labeled column)** **Strongly Disagree=1** **Disagree=2** **Neutral =3** **Agree=4** **Strongly Agree=5**	1	2	3	4	5
Moral Beliefs	Refer to an individual's judgment about engaging in ISP violation as morally wrong or right. Items adapted from Vance and Siponen (2012)	MB_1	I feel that the scenario character acted wrongly by violating company IT security policy	I would do what Jack did in the scenario.					
		MB_2	How morally wrong would it be to do what the person did in the scenario?	I feel that Jack acted wrongly by violating the company's information systems security policy.					
		MB_3	It is moral wrong to violate company information systems security policies?	It is morally wrong to do what Casey did in the scenario.					
Perceived Benefits	An estimate of the personal rewards received from complying with the required security behavior. Items adapted from Bulgurcu et al. (2010)	PBC_1	My compliance with the _____ requirements of the ISP would be favorable to me.	Doing the opposite of Jordan (i.e. complying with the workstation lock/lockout policy) would be favorable to me.					
		PBC_2	My compliance with the _____ requirements of the ISP would result in benefits to me.	My compliance with the workstation lock/logout policy would result in benefits to me.					
		PBC_3	My compliance with the _____ requirements of the ISP would create advantages for me.	My compliance with the workstation lock/logout policy would create advantages for me.					

Construct	Definition and Item Source(s)	Item code	Survey Question/Measurement Item	**Section One** **Please provide your level of agreement or disagreement with the following statements. (Please mark only one 'X' for each line in the labeled column)** **Strongly Disagree=1** **Disagree=2** **Neutral =3** **Agree=4** **Strongly Agree=5**	1	2	3	4	5
Perceived Benefits	An estimate of the negative effects that result from failing to comply with the required security actions. Items adapted from Bulgurcu et al. (2010)	PB_1	My noncompliance with the _____ requirements of the ISP would be harmful to me.	Violating the workstation lock/lockout like Jordan did would be harmful to me.					
		PB_2	My noncompliance with the _____ requirements of the ISP would impact me negatively.	Behaving like Jordan and violating the workstation lock/lockout policy would impact me negatively.					
		PB_3	My noncompliance with the _____ requirements of the ISP would create disadvantages to me.	My noncompliance with the workstation lock/logout policy would create disadvantages to me.					
Shame	Shame is a feeling of guilt or embarrassment if others knew of one's socially undesirable actions. Items adapted from Vance and Siponen (2012)	S_1	How likely is it that you would be ashamed if coworkers knew that you had violated company information security policy?	How likely is it that you would be ashamed if coworkers knew that you did what Jack did in the scenario?					
		S_2	How likely is it that you would be ashamed if others knew that you had violated the company information security policy?	How likely is it that you would be ashamed if others knew that you did what Casey did in the scenario?					

Construct	Definition and Item Source(s)	Item code	Survey Question/Measurement Item	Section One Please provide your level of agreement or disagreement with the following statements. (Please mark only one 'X' for each line in the labeled column) Strongly Disagree=1 Disagree=2 Neutral =3 Agree=4 Strongly Agree=5	1	2	3	4	5
	Items adapted from Bulgurcu et al. (2010)	S_3	How likely is it that you would be ashamed if managers knew that you had violated the company information security policy?	How likely is it that you would be ashamed if managers knew that you did what Jordan did in the scenario?					
	Shame is a feeling of guilt or embarrassment if others knew of one's socially undesirable actions. Items adapted from Vance and Siponen (2012)	S_4	How much of a problem would it be if you felt ashamed that co-workers knew you had violated the company information security policy?	How much of a problem would it be if you felt ashamed that co-workers knew that you did what Jack did in the scenario?					
		S_5	How much of a problem would it be if you felt ashamed that others knew you had violated the company information security policy?	How much of a problem would it be if you felt ashamed that others knew that you did what Casey did					
		S_6	How much of a problem would it be if you felt ashamed that managers knew you had violated the company information security policy?	How much of a problem would it be if you felt ashamed that managers knew you did what Jordan did?					

Construct	Definition and Item Source(s)	Item code	Survey Question/Measurement Item	Section One Please provide your level of agreement or disagreement with the following statements. (Please mark only one 'X' for each line in the labeled column) Strongly Disagree=1 Disagree=2 Neutral =3 Agree=4 Strongly Agree=5	1	2	3	4	5
Formal sanction	A perception that organizational punishment will be imposed. Items adapted from Siponen & Vance (2010)	FS_1	What is the likelihood you would receive sanctions if you violated the company information security policy?	My organization will discipline employees, like Jordan, who fail to follow the workstation lock/logout requirements of ISP.					
		FS_2	What is the likelihood that you would be formally sanctioned if management learned that you had violated company information security policy?	My organization will terminate employees who repeatedly fail to follow the workstation lock/logout requirements of the ISP.					
		FS_3	What is the likelihood that you would be formally reprimanded if management learned you had violated company information security policy?	If I were caught doing what Jordan did, I would be severely punished.					
	Formal sanction: A perception that organizational punishment will be harsh. Items adapted from	FS_4	How much of a problem would it be if you received severe sanctions if you violated the company information security policy?	My organization will discipline employees, like Jordan, who fail to follow the workstation lock/logout requirements of ISP.					

Construct	Definition and Item Source(s)	Item code	Survey Question/Measurement Item	**Section One** **Please provide your level of agreement or disagreement with the following statements. (Please mark only one 'X' for each line in the labeled column)** **Strongly Disagree=1** **Disagree=2** **Neutral =3** **Agree=4** **Strongly Agree=5**	1	2	3	4	5
	Siponen & Vance (2010)	FS_5	How much of a problem would it create in your life if you were formally sanctioned for doing what [the scenario character] did?	My organization will terminate employees who repeatedly fail to follow the workstation lock/logout requirements of the ISP.					
		FS_6	How much of a problem would it create in your life if you were formally reprimanded for doing what [the scenario character] did?	If I were caught doing what Jordan did, I would be severely punished.					
Informal Sanctions	A perception that punishment from friends and peers will be imposed. Items adapted from Siponen & Vance (2010)	IS_1	How likely is it that you would lose the respect and good opinion of your coworkers for violating the company information security policy?	How likely is it that you would lose the respect and good opinion of your coworkers for violating the company **USB drive policy**?					
		IS_2	How likely is it that you would jeopardize your promotion prospects if management learned that you had violated company information security policy?	How likely is it that you would jeopardize your promotion prospects if management learned that you had violated company computer virus report policy?					

Construct	Definition and Item Source(s)	Item code	Survey Question/Measurement Item	**Section One** **Please provide your level of agreement or disagreement with the following statements. (Please mark only one 'X' for each line in the labeled column)** **Strongly Disagree=1** **Disagree=2** **Neutral =3** **Agree=4** **Strongly Agree=5**	**1**	**2**	**3**	**4**	**5**
		IS_3	How likely is it that you would lose the respect and good opinion of your manager, if management learned that you had violated company IT security policies?	How likely is it that you would lose the respect and good opinion of your manager, if management learned that you had violated company Sharing customer information policies?					
Informal Sanctions	A perception that punishment from friends and peers will be harsh. Items adapted from Siponen & Vance (2010)	IS_4	How much of a problem would it create in your life if you lost the respect and good opinion of your coworkers for violating the company information security policy?	How much of a problem would it create in your work life if you lost the respect and good opinion of your coworkers for violating the company password sharing policy?					
		IS_5	How much of a problem would it create in your life if you jeopardized your future job promotion prospects for violating the company information security policy?	How much of a problem would it create in your life if you jeopardized your future job promotion prospects for violating the company password sharing policy?					

Construct	Definition and Item Source(s)	Item code	Survey Question/Measurement Item	Section One Please provide your level of agreement or disagreement with the following statements. (Please mark only one 'X' for each line in the labeled column) Strongly Disagree=1 Disagree=2 Neutral =3 Agree=4 Strongly Agree=5	1	2	3	4	5
		IS_6	How much of a problem would it create in your life if you lost the respect of your manager for doing what Aleksa did?						
Scenario type	**Adapted from Vance and Siponen (2012)**		**Which of the five scenarios do you received?**	**Please circle the scenario number**	**1**	**2**	**3**	**4**	**5**
Intention (INT)		**Self-reported intention to perform a security-related behavior. Items adapted from**	**I intend to comply with the _____ requirements of the ISP of my organization in the future.**	**It is likely that I would probably do what Jordan did in the described scenario.**					
			I intend to protect information and technology resources according to the _____ requirements of the ISP of my organization in the future.	I would act in the same way as Casey did if I were in the same situation.					
			I intend to carry out my _____ responsibilities prescribed in the ISP of my organization when I use information and technology in the future.	**If I experienced similar circumstances as Jack, I would probably operate in a similar manner.**					

9. APPENDIX II: Informed Consent Form for the Respondents

Informed Consent Form

ADDIS ABABA UNIVERSITY IT DOCTORAL PROGRAM

Informed Consent for Participants in Research Projects

Title of Study: Moderating Effect of Organizational Culture on Information Security Policy Compliance in Ethiopia: Investigating the Moderating Role of Organizational Culture

Principal Investigators:

Kibrom Tadesse,	Dr. Tilahun Muluneh, Addis Ababa University	Prof. Mikko Siponen , mikko.t.siponen@jyu.fi
Ph.D. Candidate	tilahunmuluneh@gmail.com	University of Jyväskylä
kibromtadesse@gmail.com	+251911935006	+358 505588128
+251911355996		

Study Purpose: The purpose of this survey is to gather data for academic research on Information Security Policy Compliance in Ethiopia. Specifically, we aim to investigate the moderating role of organizational culture on ISP. Your participation will contribute to our understanding of decision-making processes regarding ISP compliance/violation.

Description of Procedures: Participants will be asked to fill out a questionnaire consisting of survey questions related to ISP compliance/violation and organizational culture. The questionnaire should be completed honestly and to the best of your ability.

Duration of Study: Your participation in this study will involve completing the questionnaire, which should take approximately 15 min.

Potential Risks: There are no personal risks associated with participating in this study. However, if you experience any discomfort or have concerns while completing the questionnaire, you may stop at any time.

Potential Benefits: Your participation will contribute to academic research aimed at enhancing our understanding of ISP compliance/violation and organizational culture, which may ultimately benefit organizations and society as a whole.

Confidentiality: Your responses will be kept strictly confidential. Only the researchers listed above will have access to the data, and all identifying information will be removed to ensure anonymity.

Voluntary Participation: Your participation in this study is voluntary. You are under no obligation to participate, and you may withdraw at any time without penalty.

Contact Information: If you have any questions, concerns, or require further clarification about the study, you may contact:

Kibrom Tadesse: +251911355996

Tilahun Muluneh: +251911935006

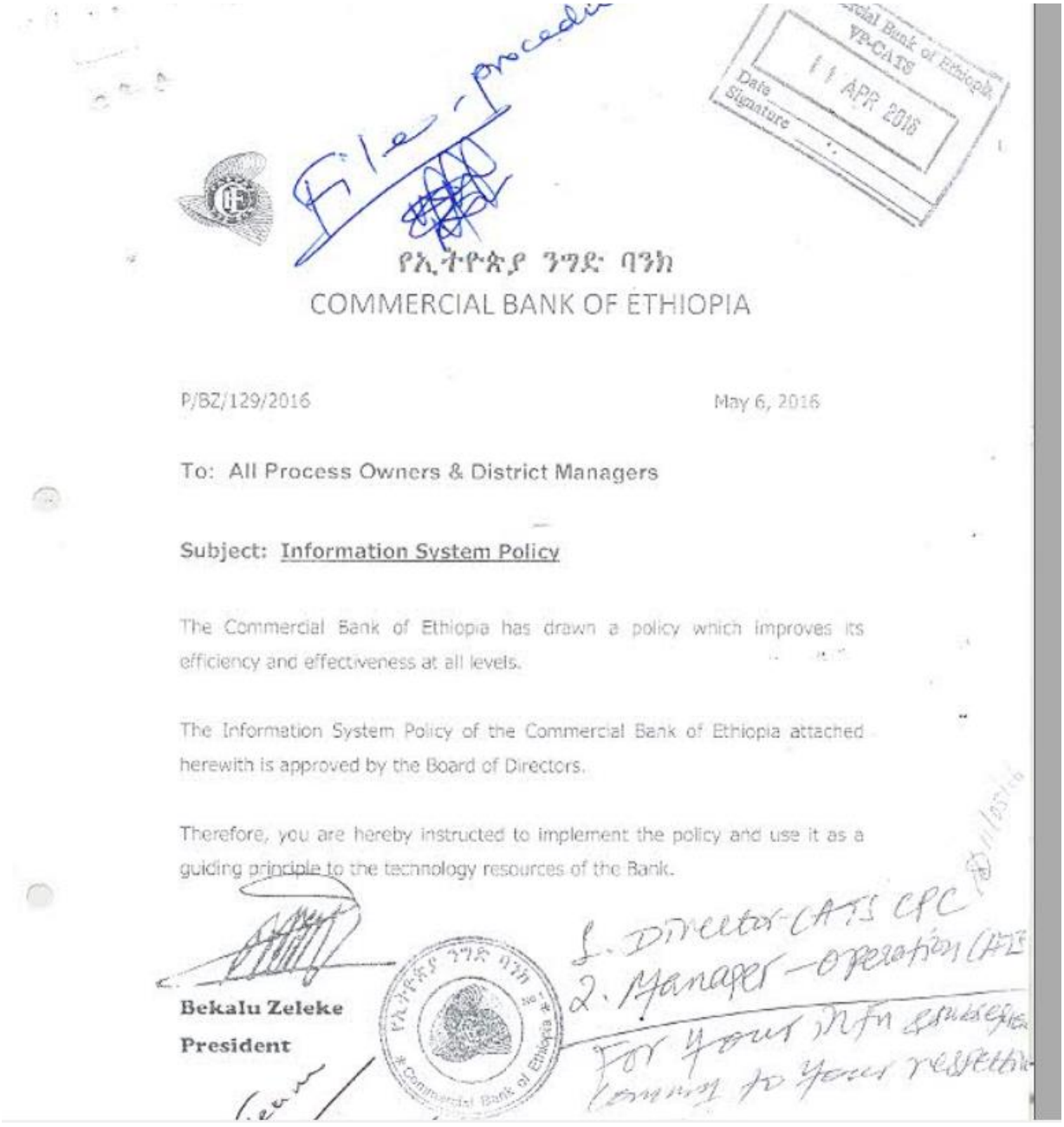
Statement of Consent: By proceeding to fill out the questionnaire, you indicate that you have read and understood the information provided above, and you voluntarily consent to participate in this study.

Please proceed to fill out the questionnaire. Your contribution to this research is greatly appreciated. Thank you for your participation.

Participant's Signature: _____

Date: _____

10. APPENDIX III: Sample ISP from Commercial Bank of Ethiopia



የኢትዮጵያ ንግድ ባንክ
COMMERCIAL BANK OF ETHIOPIA

P/BZ/129/2016 May 6, 2016

To: All Process Owners & District Managers

Subject: Information System Policy

The Commercial Bank of Ethiopia has drawn a policy which improves its efficiency and effectiveness at all levels.

The Information System Policy of the Commercial Bank of Ethiopia attached herewith is approved by the Board of Directors.

Therefore, you are hereby instructed to implement the policy and use it as a guiding principle to the technology resources of the Bank.

Bekalu Zeleke
President

01 JUN 2016
Date
Signature

የኢትዮጵያ ንግድ ባንክ
COMMERCIAL BANK OF ETHIOPIA
Interdepartmental Memorandum

P/BZ/143/2016 May 31, 2016

To: All Process Owners

Subject:- Approval of Information System Security Policy

The Board of Directors at its regular meeting held on the 11th of April 2016, deliberated on and approved *Information System Security Policy of the Bank.*

This is, therefore, to communicate the policy which came into effect as of the 11th of April 2016 for proper notation and compliance.

Bekalu Zeleke
President