SINET: Ethiop. J. Sci., 47(1): 17-32, 2024 ISSN: 0379–2897 (PRINT)
 eISSN: 2520–7997

Date received: May 2023; Date revised: April 2024; Date accepted: -August 2024
DOI: https://dx.doi.org/10.4314/sinet.v47i1.2

The Impact of Organizational Culture on Information Security Policy Compliance

Kibrom Ejigu*, Mikko Siponen and Tilahun Muluneh

College of Natural and Computational Sciences, Addis Ababa University, Ethiopia. E-mail: Kibrom.Ejigu@aau.edu.et

ABSTRACT: The objective of this study is to explore how organizational culture affects employee compliance with information security policies. To accomplish this goal, the authors developed a theoretical model and collected survey data from employees who work in organizations that have information security policies. We employed a quantitative survey research approach. We conducted our study at the commercial bank of Ethiopia (CBE). The collected data was analysed using analysis of moment structures (Cardoso and Ramos) software. The findings show that organizational culture significantly affects employee compliance with information security policies. Additionally, the study emphasizes the importance of considering the dominant organizational culture when trying to embed an information security policy. The contribution of this study lies in providing empirical evidence of the influence of organizational culture on information security compliance. To limit the scope of the study, the sample used in this research focuses only on organizational factors in Ethiopia. It is recommended that future studies be conducted in other countries to validate the results and ensure the generalizability of the findings. Practically speaking, creating a culture that supports information security practices is crucial for organizations, as technical and management measures alone cannot fully address the human aspect of information security. To better understand and enhance organizational behaviour regarding information security, companies should examine their organizational culture and how it impacts the effectiveness of implementing information security policies.

Keywords/Phrases: information security, information security compliance, organizational culture, developing country, information security compliance model, competing values framework

INTRODUCTION

The importance of information as a crucial resource for organizations has led to the development of information systems to manage their resources. These systems are interconnected globally to facilitate the quick processing and sharing of information, but this connectivity also exposes organizations to various security threats. These threats can occur during the storage, processing, and communication of information. To maintain the safety of information, organizations must implement comprehensive security mechanisms at all levels of information management(Bulgurcu et al., 2010). Although there is an increasing awareness of the benefits of information system security, most security threats come from the unintentional or intentional actions of employees. Studies show that over 80% of security threats come from insiders, and this is mainly due to the lack of knowledge about information security policies implemented in organizations(Alotaibi et al., 2016) .This lack of awareness leads to a disregard for security policies and procedures, which can result in significant consequences and damage(Bulgurcu et al., 2010; Kim and Solomon, 2016).

Information security protection mechanisms can be categorized into technical and behavioural solutions. Technical solutions include the use of passwords, access rights, intrusion detection and prevention systems, and firewalls, among others, while behavioural solutions comprise the development of information security policies, training and awareness programs, and risk monitoring. Some organizations also use punishment and rewards as behavioural solutions to encourage compliance and discourage violations of information security prevention mechanisms(Assefa, 2021; Ejigu et al., 2021). To provide a comprehensive solution to information security, organizations develop and implement information security policies (ISP).

ISP serves as a formal document that establishes guidelines, procedures, and standards for user behaviour when accessing organizational information and IT resources. It is

*Author to whom correspondence should be addressed.

crucial for ensuring the security of information resources and technological devices within an organization(Alotaibi et al., 2016; Amankwa et al., 2018). However, despite the existence of clear ISP guidelines, employees often encounter challenges adhering to the policies outlined in the document(Alotaibi et al., 2016; Bulgurcu et al., 2010).

To fill gaps in the literature, researchers must look into the relationship between organizational culture and employee compliance with information security policies. While earlier research has looked at a variety of factors that influence compliance behaviours (Arage et al., 2015; Assefa, 2021; Bulgurcu et al., 2010), the impact of organizational culture on compliance has received less attention(Ejigu et al., 2021). Besides, several researchers have suggested that further investigation is necessary to explore the relationship between organizational culture and its impact on employee information security policy compliance behaviour(Solomon and Brown, 2021; Tang et al., 2016). This research aims to fill this gap by examining the role of organizational culture in predicting and promoting information security compliance among employees. By identifying the unique contributions of organizational culture in shaping compliance behaviour, this study will provide valuable insights for practitioners seeking to enhance information security practices within their organizations.To tackle the research issue at hand, the subsequent research inquiries have been formulated:RQ1: How does organizational culture influence employees' compliance with information security policies?

The article's structure begins with an introduction to the research topic. The second section then provides a brief Literature Review of current research and knowledge gaps. The third section then presents the Conceptual Framework, which serves as the study's foundation. Then, in the fourth section we present our hypotheses. The fifth section then describes our research methods. The sixth section then presents empirical findings. The seventh section then discusses the research implications. Finally, the article discusses limitations and future research directions.

Literature Review

Information Security Policy Compliance

Information security compliance relates to the extent to which employees adhere to the rules and guidelines outlined in an organization's information security policy while using the organization's information system (Ifinedo, 2014; Siponen et al., 2010). Compliance with the ISP entails using the information system in line with established guidelines when communicating with colleagues within and outside the organization (Bulgurcu et al., 2010). It signifies the effectiveness of the implemented information security policy and procedures, while noncompliance indicates a lack of acceptance of the policy. It is important for an organization's information security policy to be designed in a way that does not create obstacles for employees in carrying out their daily tasks(Antoniou, 2015). Information security policies establish the standards and guidelines for organizations to safeguard their sensitive data and information assets(Cram et al., 2017). These policies depend on employee compliance for their effectiveness (Stafford et al., 2018). Research shows that employees often violate these policies, driven by a perception of increased productivity(Tarafdar et al., 2014). This non-compliance poses challenges to an organization's efforts to maintain robust information security(Xu et al., 2019), even with advanced security measures and well-crafted policies. Therefore, a deeper understanding of compliance behaviour within an organizational context is crucial(Ifinedo, 2014), as it helps recognize the factors influencing employee information security compliance(Hu et al., 2012).

Organizational Culture and Compliance

According to De Witte and Van Muijen (1999), organizational culture consists of shared values and beliefs that influence employee behaviour and actions within an organization. It includes deeply ingrained norms, values, and customs guiding interactions, decisions, and contributions within the organization.Research has explored the relationship between organizational culture, information security and compliance. Embedding policies in the culture has been advocated for promoting compliance. Organizational culture has been deemed a more effective driver of compliance change than traditional policing(Vroom and von Solms, 2004). Incorporating corporate governance and information security policies into the culture, with senior management involvement, has been stressed(Von Solms, 2006).

According to Karlsson et al. (2022), the aspects of organisational culture and information

security policy compliance have been addressed to a very small degree in the current literature. However, the studies byErnest Chang (2007),Hu et al. (2012), Solomon and Brown (2021), Karlsson et al. (2022)are valuable exceptions.

While prior research has examined the relationship between organizational culture and information security, there is a notable research gap and inconclusive findings regarding the effects of specific cultural orientations on employee compliance with information security measures. Ernest Chang (2007) conducted a study exploring the influence of various organizational culture traits on information security management's effectiveness, focusing on constructs like confidentiality, integrity, availability, and accountability. Their findings revealed a positive correlation between consistency and effectiveness cultures and the principles of information security management. However, it is important to note that their study did not investigate employee compliance with information security measures. Similarly, Donahue (2011) conducted a survey of information security managers within US organizations, shedding light on the impact of cultures emphasizing cooperativeness and innovativeness. Yet, it's worth highlighting that Donahue's study did not specifically address employee compliance with information security measures.

Hu et al. (2012) narrowed their focus to only two cultural orientations outlined in the competing values framework (CVF) consistency and effectiveness, examining how these orientations influence individuals' cognitive beliefs regarding information security policies. Solomon and Brown (2021)research emphasized the direct impact of an effectiveness culture on compliance, while notably; they did not find a significant impact of a consistency culture on compliance. Further adding to the complexity of findings, Karlsson et al. (2022)discovered that employees perceiving their organizations as having both consistency and cooperativeness cultures demonstrated a positive influence on information security policy compliance. These inconsistent findings highlight the need for a more comprehensive exploration of how organizational culture interacts with compliance, particularly concerning employees' adherence to information security measures. This research gap underscores the importance of investigating the intricate dynamics between specific cultural orientations and compliance behaviour, offering a more nuanced understanding of this relationship.

Conceptual Framework

Competing Values Framework:

` The literature explores various dimensions within research on information security and organizational culture, including Schein's model and Hofstede's six-dimensional framework. However, we chose the CVF model, as used in prior research(Ernest Chang, 2007; Hu et al., 2012; Karlsson et al., 2022; Solomon and Brown, 2021), for several compelling reasons. Schein's model, widely used but criticized for vague definitions, oversimplification, and neglect of external factors, Hofstede's framework, while valuable, did not measure culture individual level and oversimplifies diversity(Karjalainen et al., 2013; Vance et al., 2020). In contrast, the CVF offers a more nuanced, flexible, and context-specific approach, accommodating the complexities of real-world organizational dynamics and diverse cultural contexts. Besides, the CVF model, widely employed in organizational culture research(O'Neill et al., 2021), comprises four culture types: effectiveness, consistency, cooperativeness, and innovativeness, supported by the organizational culture assessment instrument (OCAI), utilized in over 1,000 organizations, indicating organizational success(O'Neill et al., 2021; Zeb et al., 2021). We select the CVF for its integration and organization of proposed dimensions based on empirical evidence. Our research delves into the effects of all CVF components to enhance our understanding of organizational culture's role in information security compliance. Subsequent sections provide comprehensive definitions of each component in our model.

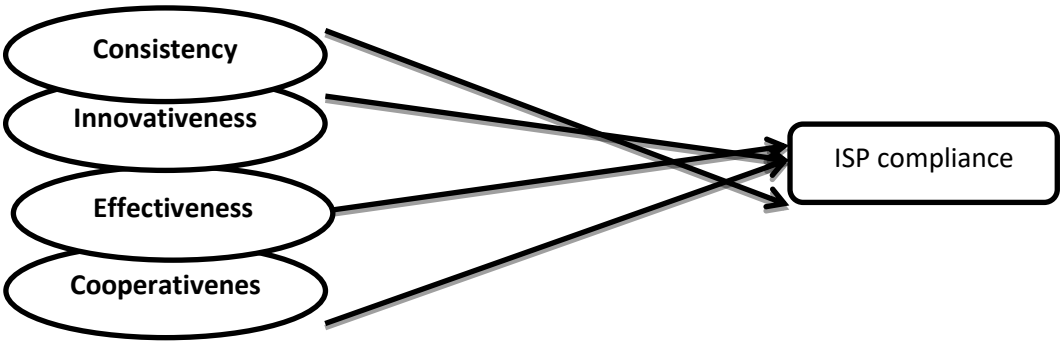


Figure 1: Research Model of ISP Compliance Source: adapted from Ernest Chang and Lin (2007).

Hypotheses

Consistency culture

The consistency culture is based on the values of efficiency, reliability, predictability, and standardization through strict adherence to rules, policies, and procedures. This culture is typical of organizations with an internal focus on people dimensions and an emphasis on control that adopt centralized authority over organizational processes, respect formal hierarchy, and adhere to rules, policies, and procedures(Di Stefano et al., 2019; Ernest Chang and Lin, 2007). It is possible that this type of culture may actually have a positive influence on employees' compliance with ISP. Organizations with a consistency culture tend to have centralized authority over processes and respect for formal hierarchy, which may promote a sense of order and accountability among employees. Moreover, strict adherence to rules and procedures may actually make it easier for employees to understand and comply with ISP requirements. Additionally, the lack of discretion among employees throughout hierarchical levels may make it easier for organizations to ensure consistent and uniform compliance with ISP requirements(Ejigu et al., 2021).

While our initial hypothesis one proposed a positive influence of consistency culture on employees' ISP compliance, empirical research reveals a complex landscape. Studies by Hu et al. (2012) and Solomon and Brown (2021)indicate a lack of direct association between consistency culture and compliance intentions, raising questions about the extent of its influence. It's worth noting that the empirical evidence isn't entirely conclusive. In contrast, Karlsson et al. (2022)found a positive impact of consistency cultures on information security policy compliance. These diverse findings highlight the need to explore contextual nuances and conditions that comprehensively determine the relationship between consistency culture and compliance. Subsequent sections will delve into these variations, examining potential contributing factors and offering a nuanced perspective on organizational culture's role in shaping compliance behaviours. Therefore, the following hypothesis is posited:

H1: Consistency culture has a positive influence on employees' compliance with the ISP.

Innovativeness Culture

An innovative culture is characterized by a focus on flexibility and innovation in order to satisfy stakeholders' needs. However, it places a greater emphasis on creativity and experimentation to drive growth and improvement. The leadership style in an innovative culture is often inventive and risk-taking, encouraging employees to explore new ideas and take calculated risks(Di Stefano et al., 2019; Ernest Chang and Lin, 2007).

Research has shown that organizations with an innovative culture are more likely to have higher levels of organizational commitment, intention to stay, and information system service quality. In an innovative culture, individuals are motivated to pursue innovation and change by investing their efforts and realizing the benefits that come with it(Di Stefano et al., 2019; Tadesse et al., 2021). This type of culture may also support the social exchange rule of reciprocity by promoting mutual reinforcement between parties(Di Stefano et al., 2019).

We argue that the emphasis on creativity, risk-taking, and open communication in an innovative culture may positively influence employee compliance with ISP policies. According to Jin and Drozdenko

(2010)employees in an innovative culture may feel a sense of ownership and empowerment, which could lead to a greater sense of responsibility and accountability in adhering to ISP policies. In a study conducted by Karlsson et al. (2022)it was found that employees who perceive their organizations as having an innovative culture had a negative impact on information security policy compliance. This intriguing contradiction prompts us to delve deeper into the complex interplay of organizational culture and compliance. While our hypothesis emphasizes the potential benefits of an innovative culture in fostering a proactive attitude toward compliance, the findings byKarlsson et al. (2022) raise questions about the conditions under which such cultures may have divergent effects.

Therefore, we propose that an innovative culture may lead to greater employee compliance with ISP policies due to its focus on innovation, experimentation, and risk-taking, which may foster a more proactive and positive attitude towards compliance. Therefore, the following hypothesis is posited:

H2: Innovation culture has a positive influence on employees' compliance with ISP.

Effectiveness culture

The effectiveness culture emphasizes the values of efficiency, goal achievement, and accountability through strict adherence to performance standards and objectives. Employees in these organizations are driven to be results-oriented, taking initiative and valuing achievement; the prevalent leadership style is directive and focused on outcomes. Research suggests that high effectiveness cultures are positively associated with organizational commitment, job involvement, job satisfaction, trust, and empowerment and negatively associated with conflict and resistance to change(Di Stefano et al., 2019).

This culture is typical of organizations with a focus on customer satisfaction and an emphasis on performance that adopt decentralized authority over organizational processes, respect results-based hierarchy, and emphasize accountability. According to Kakkar and Sivanathan (2022)a culture that values achievement and accountability may actually reduce the likelihood of unethical behaviours such as violations of ISP, as employees are more likely to be committed to the organization's goals and values. We argue that an effective culture, due to its focus on accountability and results, could actually influence employee compliance with ISP policies.

While our hypothesis posits a positive influence of an effectiveness culture on employees' compliance with ISP policies, the empirical landscape reveals mixed findings. Hu et al. (2012) did not establish a direct association between effectiveness culture and compliance, suggesting a more complex relationship. In contrast,Solomon and Brown (2021) support our hypothesis, showing a positive impact of an effectiveness culture on compliance. However, Karlsson et al. (2022) present a contrasting perspective, indicating a negative impact of an effectiveness culture on information security policy compliance. These mixed findings emphasize the need for a comprehensive exploration of the influence of organizational culture on compliance and consideration of potential moderating factors.

In subsequent sections, we will delve into these variations, examine contextual nuances, and aim to provide a nuanced understanding of the effectiveness culture's relationship with compliance. Thus, the following hypothesis is posited:

H3: Effectiveness culture has a positive influence on employees' compliance with ISP.

Cooperativeness Culture

A cooperative culture, also known as a collaborative culture, places a high value on teamwork and group efforts to achieve common goals. The leadership style is supportive and focused on employee empowerment and participation. This type of culture emphasizes employee involvement, cohesion, and mutual support and is characterized by a sense of belonging and loyalty to the organization. Research has shown that this type of culture is positively related to organizational commitment, job satisfaction, and trust(Goodman et al., 2001).

In this culture, employees are encouraged to engage in prosaic behaviours and organizational citizenship behaviours, which can positively impact their compliance with ISP policies. According to the exchange norm of group gain, individuals are expected to act in the interest of the group, and behaviours that are damaging to the collective are strongly discouraged(Di Stefano et al., 2019; Tadesse et al., 2021). Hence, it is reasonable to expect that employees in cooperative cultures are less likely to engage in ISP non-compliance.

Furthermore, research has shown that organizations that promote collaboration and

teamwork are more likely to have a positive ethical climate, which is characterized by a shared belief in the importance of ethical behaviour (Di Stefano et al., 2019). Such ethical climates can help reinforce the importance of ISP compliance and create a sense of shared responsibility for maintaining the security of information systems. According toKarlsson et al. (2022), the cooperativeness culture that employees believe exists at their organisations has a positive effect on their compliance with information security policies.Therefore, we hypothesize that cooperativeness culture has a positive influence on employees' compliance with ISP, as it promotes pro-social and organizational citizenship behaviours, reinforces the exchange norm of group gain, and fosters a positive ethical climate that emphasizes the importance of ISP compliance.

H4: A cooperative culture has a positive influence on employees' compliance with ISP.

Method

For our study on assessing employee compliance with information security policies, we employed a quantitative survey research approach. This choice is grounded in several key considerations: Firstly, a quantitative survey approach is well-suited for collecting data from a substantial sample population, allowing for a comprehensive analysis (Kumar, 2018). Secondly, it provides the means to precisely measure the variables related to compliance with information security policies, facilitating numerical analysis essential for our research (Bryan, 2020). Thirdly, the use of surveys ensures the objectivity and standardization of data collection as respondents provide responses to predefined questions, reducing potential bias and subjectivity(Edwards et al., 2014). Lastly, our decision is supported by the approach's ability to explore causal relationships between independent and dependent variables, a critical aspect in the investigation of employee compliance with information security policies(Mohajan, 2020).

For our study, we conducted research at the Commercial Bank of Ethiopia, recognized as one of the largest financial institutions in Ethiopia having branch offices all over the country. From all CBE branch offices, six branch offices located in Adama and Addis Ababa were selected by using random sample method. Then we compiled a list of employees who work in the selected branch offices. The list of employees was organised by department, and representative samples were drawn from each. We used systematic sampling methods to select questionnaire respondents. We used Solvin's formula to calculate the sample size.The total number of employees in six branches was 670. Of which 250 samples were selected using 5% margin error and 95% level of confidence (Kothari, 2004).

Data analysis was performed using AMOS software. AMOS software was selected for data analysis due to its robust capabilities. Its primary strengths lie in structural equation modelling Tilahun and Tibebe (2017), which is ideal for exploring complex relationships in research, such asinformation security compliance. AMOS accommodates both reflective and formative measurements, making it versatile in handling various data types. Moreover, it facilitates theory development and has high statistical power, ensuring the detection of subtle associations. The ability to conduct path analysis is crucial when exploring multiple variable relationships, and AMOS enjoys widespread acceptance in the research community, aligning with journal-level publication standards.

We employed established tools for data collection, drawn from the existing literature on information security (Table 1). To ensure the reliability and validity of our instrument, we conducted a pilot test with 50 employees from the commercial bank of Ethiopia, with 21 completing the questionnaire (42% response rate.) a group separate from the main survey to mitigate potential biases. The analysis confirmed the instrument's validity and reliability, with Cronbach's α value above .82. During the pilot test, participants reviewed the questionnaire for validity, clarity, question order, and redundancy. Feedback from the pilot test informed the final questionnaire. It comprises two sections: the first gathers demographic information, including gender, education level, and work experience, to explore potential influences on participants' perceptions and behaviours regarding information security policies. This demographic data enhances the interpretation of study results. The second section, a pivotal component, contains tools designed to directly measure the research variables, providing essential insights into the effectiveness of information security policies. We used paper-based surveys due to internet connectivity challenges.

Table 1. Measurement items for organizational culture and information security compliance.

Cooperativeness	COOP_1	Managers empower staff	Ernest Chang (2007)
	COOP_2	In this organization, managers treat all staff as their big family members.	Ernest Chang (2007)
	COOP_3	Employees are loyal and trust one another.	Ernest Chang (2007)
	COOP_4	Your organization encourages employees to actively participate all company activities and events.	Ernest Chang (2007)
	COOP_5	Employees are devoted to protect their organization.	Ernest Chang (2007)
	COOP_6	Employees are trusted by their managers, and can participate in the decision making process.	Ernest Chang (2007)
	COOP_7	It is very harmonious amongst employees, and your company is treated like a big family.	Ernest Chang (2007)
	COOP_8	Your Company pays attentions to human resource development, employees' morale, and team work.	Ernest Chang (2007)
Innovativeness	INNO_1	Managers have courage to make innovation and take risk.	Ernest Chang (2007)
	INNO_2	Managers actively lead the staff to grow and innovate.	Ernest Chang (2007)
	INNO_3	Managers have vision and insights to create new business opportunities.	Ernest Chang (2007)
	INNO_4	Employees always have to face challenges and they can learn and grow from the challenges.	Ernest Chang (2007)
	INNO_5	Your Company pays attentions to the uniqueness of employees and encourages the innovation from employees.	Ernest Chang (2007)
	INNO_6	Your Company is willing to take risks, and it is indeed an ambitious and energetic organization.	Ernest Chang (2007)
Consistency	CONS_1	Managers set up clear goals and demand employees to carry out the goals strictly.	Ernest Chang (2007), Hu et al. (2012).
	CONS_2	Your Company always has formal and strict rules for employees to follow.	Ernest Chang (2007), Hu et al. (2012).
	CONS_3	The operation of your company emphasizes stability and conservative culture. It does not allow any confusion.	Ernest Chang (2007), Hu et al. (2012)
	CONS_4	Your Company pays attentions to efficiency and performance for achieving the goals.	Ernest Chang (2007), Hu et al. (2012)
	CONS_5	Your Company is stable and offers job security to employees.	Ernest Chang (2007), Hu et al. (2012)
	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.	Ernest Chang (2007), Hu et al. (2012)
Effectiveness	EFFE_1	Managers emphasize working efficiency and acts effectively.	Ernest Chang (2007), Hu et al. (2012)
	EFFE_2	Managers pay attentions to achieve good work performance and reach the goal, regardless of personal feelings.	Ernest Chang (2007), Hu et al. (2012)
	EFFE_3	The critical success factor of your company is its good productivity.	Ernest Chang (2007), Hu et al. (2012)
	EFFE_4	Your Company pays attentions to work efficiency. Every department and	Ernest Chang (2007), Hu et al. (2012)
	EFFE_5	Your Company pays attentions to maintaining its competition advantages.	Ernest Chang (2007), Hu et al. (2012)
	EFFE_6	Your Company pays attentions to employees in terms of increasing their efficiency and pursuing their accomplishment.	Ernest Chang (2007), Hu et al. (2012)
Information security Policy compliance	ISP_1	I follow information security policy and procedures while communicating with other colleagues within and outside the organization.	Bulgurcu et al. (2010)
	ISP_2	I protect information and technology resources according to the requirements of the information security policy of my organization.	Bulgurcu et al. (2010)
	ISP_3	I understand that information security policy is not restrictive to access information resources in my organization.	Antoniou (2015)

RESULTS

We will now delve into the outcomes of the measurement model evaluation, structural model examination, and hypothesis testing. These results adhere to the rigorous criteria expected in quantitative research within the field of information systems.

Descriptive Statistics

Out of the 250 questionnaires distributed to the selected sample, 221 were correctly completed and returned, resulting in a response rate of 88.4%, which aligns with sampling assumptions. This sample comprised 143 male respondents and 78 female respondents, indicating a somewhat skewed gender distribution. The majority of participants, constituting 52.5% of the sample, fell within the age range of 26 to 35 years. Additionally, 29.9% were aged between 36 and 45 years, while the remaining 17.6% were between 20 and 25 years old. It's important to note that no data errors were identified that could introduce gender or age bias. In terms of educational attainment, the majority of respondents (75.6%) held a bachelor's degree, followed by 19.9% with a master's degree, and 4.5% with a college diploma, indicating a well-educated participant group capable of understanding and adhering to organizational information security policies.

Further analysis based on respondents' computer experience revealed that 56.6% reported having good computer experience, 34.8% had satisfactory experience, 7.7% had sufficient experience, and 0.9% had moderate experience. This data underscores the reliance of employees on computers for information management, highlighting their susceptibility to potential information security risks. Despite the high response rate, some respondents (29) chose not to return the questionnaire, while 5 provided incomplete responses, resulting in their exclusion from the data analysis process.

Measurement Model Evaluation

The assessment of reliability and validity is a critical step in validating a measurement model. In this study, we rigorously examined the model fit measurements, reliability and validity of our measurement model by assessing construct reliability, using composite reliability (CR), average variance extracted (AVE), maximum shared variance (MSV), and maximum variance extracted (MaxR(H)). The results confirmed high internal consistency, convergent validity, and discriminant validity across all constructs. These findings demonstrate the robustness of the measurement model, thereby affirming its suitability for assessing latent constructs in the studied population. A visual representation of the measurement model is presented in Figure 2.

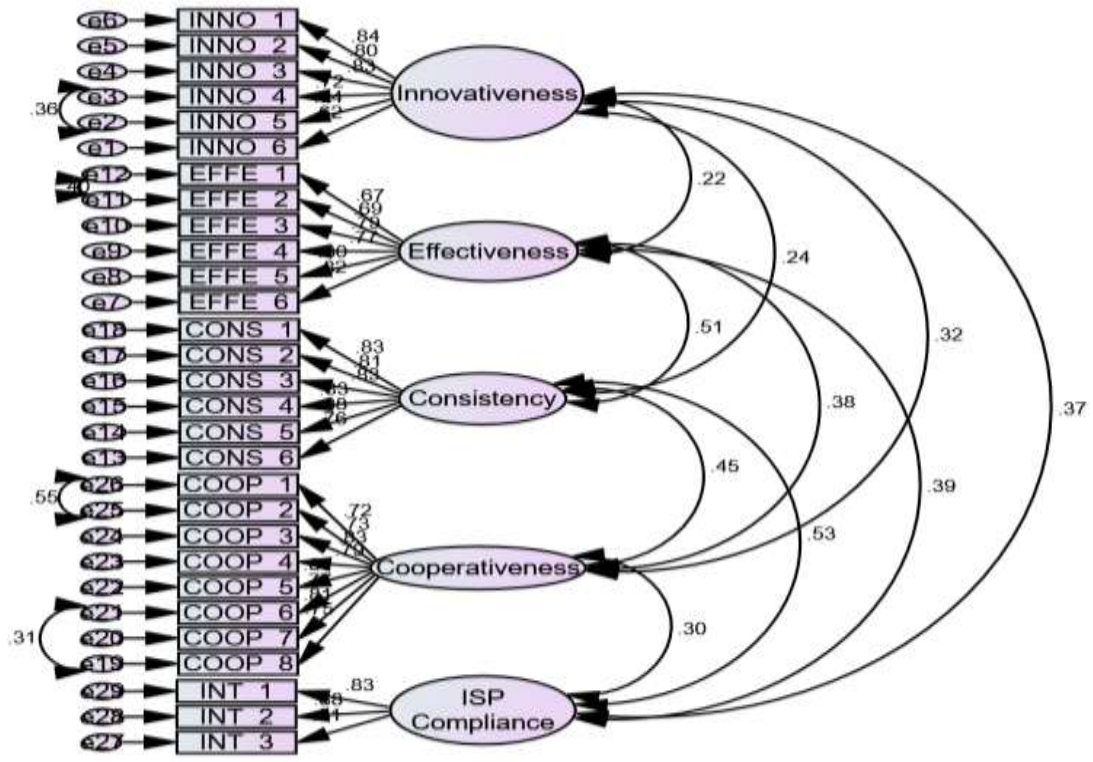


Figure 2: The Proposed Measurement Model

In structural equation modelling Tilahun and Tibebe (2017), assessing goodness of fit involves several categories of fit indices: absolute (e.g., Chi-square, RMSEA, RMSR, SRMR), incremental (e.g., CFI, NFI, TLI, IFI), relative (RFI), and parsimonious (e.g., PCFI, PRATIO, PNFI). Hair Jr et al.'s (2017) recommend using a subset of three or four fit indices: chi-square, at least one incremental, and at least one absolute fit index for a well-rounded assessment.

The model's fit assessment yielded these results: CMIN = 815.11, CMIN/DF = 2.245, RMSEA = 0.048, indicating a close fit. Incremental fit indices (CFI, IFI, TLI, NFI, RFI) all exceeded 0.9, indicating a robust fit. Parsimony fit indices (PCFI, PNFI, PRATIO) neared 1, striking a balance between fit and complexity. These results affirm the model's compatibility with the data and its ability to provide insights into variable relationships.

Table 2. Goodness of Fit Statistics for the Model.

Absolute Fit Index		Incremental Fit Index		Parsimony Fit Index	
CMIN	815.11	CFI	.958	PCFI	.857
DF	363	IFI	.958	PNFI	.829
CMIN/DF	2.245	TLI	.953	PRATIO	.894
RMSEA	0.048	RFI	.918		
PClose	0.825	NFI	.927		
SRMR	0.037				

The results, as summarized in Table 2, are as follows: Composite Reliability (CR) the assessment revealed that all constructs exhibited acceptable levels of internal consistency, with CR values ranging from 0.878 to 0.927 in line with Hair Jr et al. (2017)guidelines. This indicates the model's ability to consistently measure each construct. Convergent Validity (AVE) the AVE value, ranging from 0.576 to 0.706, demonstrated that each constructswas above the recommended threshold of 0.50 (Straub et al., 2004). Discriminant Validity (MSV and MaxR(H)): The analysis of MSV values, ranging from 0.138 to 0.279, indicated a lack of substantial overlap among the constructs, confirming discriminant validity.

Additionally, all MaxR(H) values were below the corresponding AVE values, thereby strengthening the case for convergent validity. Correlation Matrix: The correlation coefficients

presented in Table 1 between the constructs were all found to be below the AVE values, providing further evidence of discriminant validity, in accordance with the principles outlined byHair Jr et al. (2017).The results of the validity analysis underscore the robustness and reliability of the measurement model. All constructs exhibited high composite reliability, convergent validity, and discriminant validity, thereby affirming the model's quality.

Table 3. Reliability and Validity Test Result.

	CR	AVE	MSV	MaxR(H)	Innovativeness	Effectiveness	Consistency	Cooperativeness	ISP Compliance
Innovativeness	0.892	0.582	0.138	0.903	**0.763**				
Effectiveness	0.890	0.576	0.262	0.897	0.216***	**0.759**			
Consistency	0.927	0.679	0.279	0.930	0.240***	0.512***	**0.824**		
Cooperativeness	0.925	0.606	0.199	0.927	0.318***	0.379***	0.446***	**0.778**	
ISP Compliance	0.878	0.706	0.279	0.883	0.371***	0.385***	0.528***	0.304***	**0.840**

The Structural Model Evaluation

The next step in SEM analysis is to conduct statistical tests of hypotheses and verify the structural model's validity. In Table 4, we can see how well the statistical model passed the SEM test. The R-squared value and the regression weight analysis can be found in Tables 5 and 6, respectively. Several types of fit indices are used to determine whether or not a structural equation model Tilahun and Tibebe (2017)is plausible. These include absolute (e.g., Chi-square, RMSEA, SRMR) and incremental (e.g., CFI, TLI, NFI), relative (RFI), and parsimonious (e.g., PCFI, PRATIO, PNFI) fit indices. For a thorough evaluation, Hair Jr. et al. (2017) suggest using a combination of three or four fit indices, including the chi-square, at least one incremental, and at least one absolute fit index.

In our study, these measures are categorized into three types: absolute fit indices, incremental fit indices, and parsimony fit indices, adhering to established criteria for each measure. These criteria, formulated by experts in the field of statistics(Hair Jr et al., 2017), furnish valuable insights into the model's overall fit, improvements over a baseline model, and model parsimony. Absolute fit indices encompass degrees of freedom (DF), Chi-square statistic (CMIN), Chi-square divided by degrees of freedom (CMIN/DF), root mean square error of approximation (RMSEA), and standardized root mean square residual (SRMR).

The CMIN value, at 815.11, is associated with 363 degrees of freedom. The CMIN/DF ratio, at 2.24, falls within the recommended range of 1 to 3, signifying a good fit. The RMSEA, measuring 0.048, is below the suggested threshold of 0.06, indicating a robust model fit. The SRMR, with a value of 0.037, is also below the recommended threshold of 0.08, denoting excellent fit. Consequently, the model demonstrates an excellent fit, providing valuable insights into model performance. The results affirm the model's strong fit and its ability to elucidate relationships among variables within the model.

Table 4. Model Fit indices for the structural model.

Absolute Fit Index		Incremental Fit Index		Parsimony Fit Index	
CMIN	815.11	CFI	.958	PCFI	.857
DF	363	IFI	.958	PNFI	.829
CMIN/DF	2.24	TLI	.953	PRATIO	.894
RMSEA	0.048	RFI	.918		
PClose	0.825	NFI	.927		
SRMR	0.037				

The output presented in Table 5 showcases the standardized regression weights between latent constructs and their respective observed variables, providing compelling grounds for the research. The regression weights offer crucial insights into the strength and direction of the relationships investigated, underscoring the significance of the research findings. The regression weights reveal substantial and consistent associations between the latent constructs and their observed variables. For instance, the regression weights between innovativeness (INNO) and its observed variables (INNO_1, INNO_2, INNO_3, INNO_4, INNO_5, and INNO_6) consistently range from.722 to.837. This indicates a robust and positive relationship between innovativeness and its indicators, implying that higher levels of innovativeness correspond to higher scores on the observed variables. Likewise, the relationships between effectiveness (EFFE) and its observed variables (EFFE_1, EFFE_2, EFFE_3, EFFE_4, EFFE_5, and EFFE_6) demonstrate consistent positive associations, with regression weights ranging from.755 to.822.

This consistent pattern validates the relationship between effectiveness and its indicators, offering valuable insights into the research question. Furthermore, the relationships between consistency (CONS) and its observed variables (CONS_1, CONS_2, CONS_3, CONS_4, CONS_5, and CONS_6) display a strong positive connection, with regression weights ranging from.759 to.881. This consistent pattern further supports the robustness of the relationship between consistency and its indicators, providing compelling evidence for the research's objectives. Similarly, the associations between cooperativeness (COOP) and its observed variables (COOP_1, COOP_2, COOP_3, COOP_4, COOP_5, COOP_6, COOP_7, and COOP_8) consistently exhibit positive relationships, with regression weights ranging from.717 to.813.

These findings reinforce the validity of the relationship between cooperativeness and its indicators, contributing to the understanding of the research area. Moreover, the relationship between ISP compliance (INT) and its observed variables (INT_1, INT_2, and INT_3) demonstrates a strong positive association, with regression weights ranging from.811 to.881. This finding provides valuable insights into the relationship between ISP compliance and its indicators, contributing to the knowledge base in the field. The consistent and significant regression weights presented in the analysis strongly support the research hypotheses and objectives.

The analysis of standardized regression weights between latent constructs and their corresponding observed variables is a fundamental aspect of SEM. Such an analysis serves as a cornerstone for evaluating the robustness of relationships within the model, shedding light on the strength and direction of these connections. The significance of this analysis lies in its potential to validate research findings and contribute to a deeper understanding of the phenomena under investigation. In this study, we delve into the intricate web of relationships between latent constructs and their observed indicators, emphasizing the importance of these connections in our research. Through the examination of standardized regression weights, we aim to uncover consistent and substantial associations, which hold the key to unravelling our research's implications.

To illustrate the significance of this analysis, the output in Table 5 presents standardized regression weights between latent constructs and their corresponding observed variables, emphasizing the research's significance. These regression weights offer essential insights into the strength and direction of the relationships under investigation, underscoring the research findings' importance. Notably, the consistent and substantial associations between latent constructs and their observed variables are evident. For example, innovativeness (INNO) exhibits robust and positive relationships with its indicators (INNO_1, INNO_2, INNO_3, INNO_4, INNO_5, INNO_6), with regression weights consistently ranging from.722 to.837. Similarly, effectiveness (EFFE) displays consistent positive relationships with its observed variables (EFFE_1, EFFE_2, EFFE_3, EFFE_4, EFFE_5, EFFE_6), featuring regression weights ranging from.755 to.822.

These patterns validate the relationships between latent constructs and their indicators, offering valuable insights into the research question. Furthermore, the strong positive connections between consistency (CONS) and its observed variables (CONS_1, CONS_2, CONS_3, CONS_4, CONS_5, CONS_6) are evident, with regression weights ranging from.759 to.881. These consistent findings support the relationship between consistency and its indicators, providing compelling evidence for the research's objectives. The positive associations between cooperativeness (COOP) and its observed variables (COOP_1, COOP_2,

COOP_3, COOP_4, COOP_5, COOP_6, COOP_7, COOP_8) also reinforce the validity of this relationship, contributing to a deeper understanding of the research area. Moreover, the strong positive association between ISP compliance (INT) and its observed variables (INT_1, INT_2, INT_3), featuring regression weights ranging from.811 to.881, provides valuable insights into the relationship between ISP compliance and its indicators, further enriching the field's knowledge base. These consistent and significant regression weights strongly affirm the research hypotheses and objectives.

Table 5. Factor Loadings.

Standardized Regression Weights			Estimate
INNO_6	<---	Innovativeness	.722
INNO_5	<---	Innovativeness	.744
INNO_4	<---	Innovativeness	.723
INNO_3	<---	Innovativeness	.828
INNO_2	<---	Innovativeness	.800
INNO_1	<---	Innovativeness	.837
EFFE_6	<---	Effectiveness	.822
EFFE_5	<---	Effectiveness	.798
EFFE_4	<---	Effectiveness	.767
EFFE_3	<---	Effectiveness	.795
EFFE_2	<---	Effectiveness	.755
EFFE_1	<---	Effectiveness	.773
CONS_6	<---	Consistency	.759
CONS_5	<---	Consistency	.881
CONS_4	<---	Consistency	.832
CONS_3	<---	Consistency	.825
CONS_2	<---	Consistency	.812
CONS_1	<---	Consistency	.831
COOP_8	<---	Cooperativeness	.754
COOP_7	<---	Cooperativeness	.810
COOP_6	<---	Cooperativeness	.773
COOP_5	<---	Cooperativeness	.813
COOP_4	<---	Cooperativeness	.791
COOP_3	<---	Cooperativeness	.827
COOP_2	<---	Cooperativeness	.735
COOP_1	<---	Cooperativeness	.717
INT_3	<---	ISP_Compliance	.811
INT_2	<---	ISP_Compliance	.881
INT_1	<---	ISP_Compliance	.827

The squared multiple correlations (R-squared) are a statistic used in regression analysis to measure the proportion of the variance in the dependent variable that is predictable from the independent variables. Table 6, the R-squared value for the variable "ISP_Compliance" is 0.354, which means that approximately 35.4% of the variance in the dependent variable can be explained by the independent variables in the regression model. This value indicates the goodness of fit of the regression model. A higher R-squared value suggests that the independent variables in the model explain a larger proportion of the variance in the dependent variable, while a lower R-squared value suggests that the model is not a good fit for explaining the variation in the dependent variable.

Table 6. Squared Multiple Correlations.

	Estimate
ISP_Compliance	.35

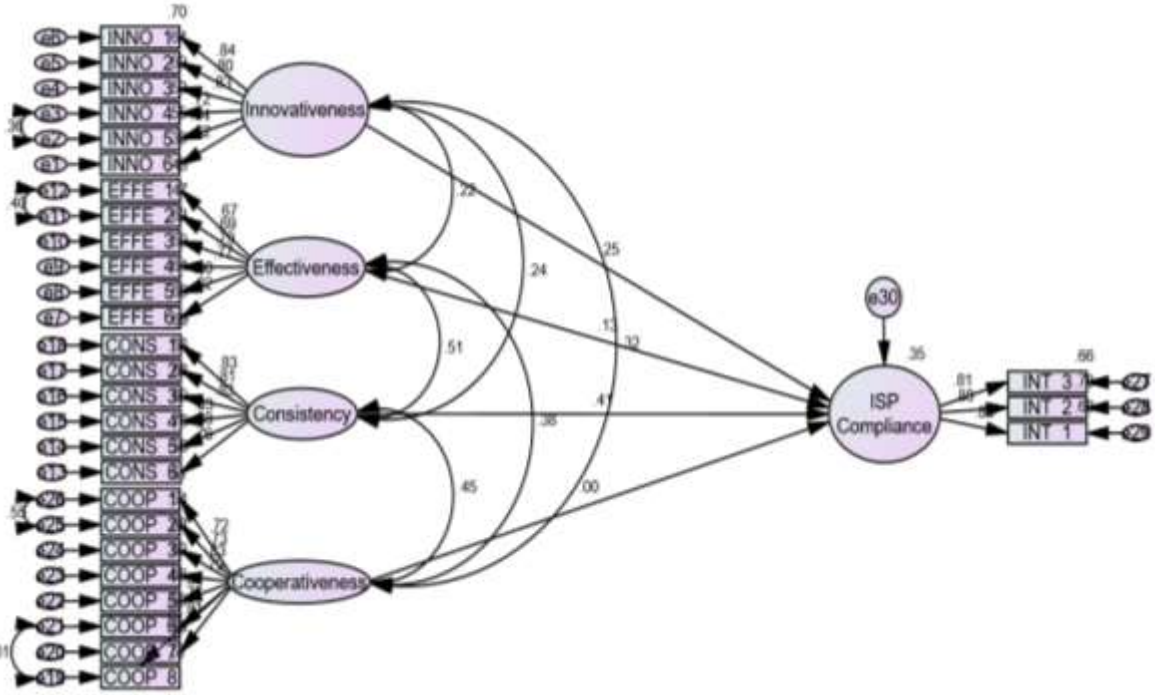


Figure 3. Goodness of Fit Statistics for the structural model.

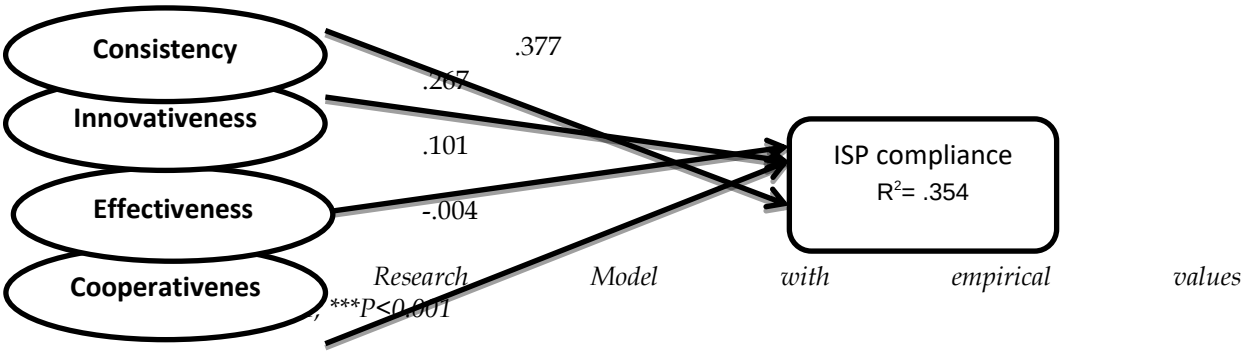
Hypotheses Testing

Our first hypothesis (H1) postulated a positive relationship between consistency culture and employees' intentions toward ISP compliance. As depicted in Table 7, the path coefficient (β) is 0.377, with a t-value of 7.541, and the p-value of less than 0.001. These statistical results support H1, with a p-value below 0.05, demonstrating statistical significance. This affirms that consistency culture positively influence on employees' ISP compliance intentions. The standardized estimate reinforces this relationship (H1: β = 0.377; t-value = 7.541; p < 0.001).Hypothesis 2 (H2) proposed a positive relationship between the innovativeness culture and employees' intentions toward ISP compliance. The results in Table 7 reveal a path coefficient (β) of 0.267, a t-value of 5.396, and a p-value of 0.001. These findings strongly support H2, with a p-value well below the significance threshold. This demonstrates that the innovativeness culture indeed exerts a positive influence on employees' ISP compliance intentions.

Our third hypothesis 3, (H3), suggested a positive relationship between effectiveness culture and employees' intentions toward ISP compliance. Table 7 presents a path coefficient (β) of 0.101, a t-value of 2.513, and a p-value of 0.012, all indicating robust statistical support for H3. This confirms that effectiveness culture have a substantial positive impact on employees' ISP compliance intentions.In relation to Hypothesis 4 (H4), the empirical examination presented in Table 7 reveals that the influence of cooperativeness culture on employees compliance intention is not statistically significant (H4: β= -0.004, t-value = -0.088, P=0.930). Thus, we can conclude that H4 is rejected, suggesting that the presence of an innovativeness culture does not have a substantial enhancing effect on employees compliance intention.

Table 7. Hypotheses results of the structural model.

Hypothesized Relationship	Standardize Estimate	t-value	P-value	Decision
ISP_Compliance <--- Consistency	.377	7.541	***	Supported
ISP_Compliance<---Innovativeness	.267	5.396	***	Supported
ISP_Compliance <--- Effectiveness	.101	2.513	.012	Supported
ISP_Compliance<---Cooperativeness	-.004	-.088	.930	Not supported



Research Model with empirical values

*, ***P<0.001*

DISCUSSION

Organizational culture's impact on employee compliance with information security policy is a critical concern. A consistent organizational culture significantly influences compliance, emphasizing the need for organizations to foster a culture that values consistent policy implementation. Clear and uniform policies and procedures are crucial to ensure employees understand and adhere to them. Managers play a pivotal role as role models, influencing compliance by providing resources. Innovation culture, characterized by creativity, experimentation, and adaptability, is the second most influential factor, contributing 26.7% to compliance. Organizations must balance innovation and compliance, empowering employees to innovate responsibly while emphasizing information security. Effectiveness culture, contributing 10.1% to compliance, emphasizes results and high-quality outcomes. However, organizations must not undervalue information security and compliance in their pursuit of results. Employees should prioritize compliance alongside their goals.

As proposed byErnest Chang (2007), information security's evolution involves technical, management, and institutionalization aspects. Top management's involvement in policy development is crucial. Organizations aim to foster an organizational culture that makes information security an integral part of every employee's tasks. Compliance with information security policies can be facilitated by information security managers. Organizations are urged to adopt an integrated approach that combines policy and organizational culture aspects. The efficiency of information security policy depends on the internal organizational culture shared by all employees at all levels.Vroom and von Solms (2004)merge organizational behaviour levels with Schein (1983)culture model, illustrating how culture influences behaviour across different organizational levels. To enhance policy compliance, organizations should explore organizational culture's influence on information security policies. The initial step to achieving information security compliance involves assessing cultural prerequisites for ISP. Subgroups within an organization may share common cultural dimensions but also develop unique sub-cultures, collectively influencing the overall culture. In summary, organizations must strike a balance between culture and compliance, shifting their culture to prioritize compliance and align it with strategic objectives to maintain a secure and compliant environment.

CONCLUSION

This study, employed survey data and structural equation modelling to examine the relationships between organizational culture and information security compliance. The aim was to identify the elements of organizational culture influencing employee compliance with information security policies. The study identified four dimensions of organizational factors: consistency, innovativeness, cooperativeness, and effectiveness. The results indicated that all factors, except cooperativeness, positively influenced employee compliance with ISP. Consistency emerged as the primary influencer, followed by innovativeness, while effectiveness had a comparatively lower impact. The existing literature lacks a comprehensive theory for analysing information security compliance.

This research contributes to theoretical knowledge by adopting an organizational culture perspective to explore factors affecting employee behaviour concerning information security compliance. Additionally, the study validates the data collection tools used to measure different dimensions of organizational culture factors related to information security

compliance. The study presents a novel model that uses CVF to explore organizational cultural impacts on employee compliance with information security policies. The research adopts an individual-level approach, addressing concerns of oversimplification and enriching the field of information system security research.

The study has limitations. It focused on a single organization in a specific country, limiting the generalizability of findings to other organizations and countries. Measuring employees' intentions rather than their actual behaviour is another limitation, though intentions are typically associated with actual behaviour. Future research recommendations include conducting similar studies in diverse geographic contexts for comparative analysis. Moreover, the research model, which explained only 35% of the variation in ISP compliance, can benefit from the incorporation of additional technical and individual factors to enhance predictive power. The study intends to expand in the future by considering these supplementary factors to create a more comprehensive model for understanding factors influencing employee behaviour regarding information security compliance.

REFERENCES

1. Alotaibi, M., et al. (2016). *Information security policies: A review of challenges and influencing factors.* Paper presented at the 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST).
2. Amankwa, E., et al. (2018). Establishing information security policy compliance culture in organizations. *Information & Computer Security*.
3. Antoniou, G. S. (2015). *Designing an effective information security policy for exceptional situations in an organization: An experimental study.* Nova Southeastern University,
4. Arage, T., et al. (2015). Influence of national culture on employees' compliance with information systems security (ISS) policies: towards ISS culture in Ethiopian companies.
5. Assefa, T. (2021). Factors influencing information security compliance: an institutional perspective. *SINET: Ethiopian Journal of Science, 44*(1), 108-118.
6. Bryan, L. L. (2020). Effective information security strategies for small business. *International Journal of Cyber Criminology, 14*(1), 341-360.
7. Bulgurcu, B., et al. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 523-548.
8. 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*.
9. Cram, W. A., et al. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems, 26*, 605-641.
10. De Witte, K. and Van Muijen, J. J. (1999). Organizational culture. *European Journal of work and organizational psychology, 8*(4), 497-502.
11. 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.
12. Edwards, M. L., et al. (2014). An experimental test of the effects of survey sponsorship on internet and mail survey response. *Public Opinion Quarterly, 78*(3), 734-750.
13. Ejigu, K. T., et al. (2021). *Investigating the Impact of Organizational Culture on Information Security Policy Compliance: The Case of Ethiopia.* Paper presented at the Americas Conference on Information Systems.
14. Ernest Chang, S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438-458. doi:10.1108/02635570710734316
15. Ernest Chang, S. and Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438-458.
16. Goodman, E. A., et al. (2001). The competing values framework: Understanding the impact of organizational culture on the quality of work life. *Organization Development Journal, 19*(3), 58.
17. 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.
18. 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.
19. 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.
20. Jin, K. G. and Drozdenko, R. G. (2010). Relationships among perceived organizational core values, corporate social responsibility, ethics, and organizational performance outcomes: An empirical study

of information technology professionals. *Journal of business ethics, 92*, 341-359.

21. Kakkar, H. and Sivanathan, N. (2022). The impact of leader dominance on employees' zero-sum mindset and helping behavior. *Journal of Applied Psychology, 107*(10), 1706.
22. Karjalainen, M., et al. (2013). One size does not fit all: different cultures require different information systems security interventions.
23. Karlsson, M., et al. (2022). The effect of perceived organizational culture on employees' information security compliance. *Information & Computer Security, 30*(3), 382-401.
24. Kim, D. and Solomon, M. G. (2016). *Fundamentals of Information Systems Security: Print Bundle*: Jones & Bartlett Learning.
25. Kothari, C. R. (2004). *Research methodology: Methods and techniques*: New Age International.
26. Kumar, R. (2018). *Research methodology: A step-by-step guide for beginners*: Sage.
27. 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.
28. O'Neill, D., et al. (2021). Leadership and community healthcare reform: a study using the Competing Values Framework (CVF). *Leadership in Health Services, 34*(4), 485-498.
29. Schein, E. H. (1983). Organizational culture: A dynamic model.
30. Siponen, M., et al. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64-71.
31. 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.
32. Stafford, T., et al. (2018). The role of internal audit and user training in information security policy compliance. *Managerial Auditing Journal, 33*(4), 410-424.
33. Tadesse, K., et al. (2021). Influence of Organizational Culture on Employees' Compliance with Information Security Policy: Ethiopian and Finland Companies.
34. Tang, M., et al. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management, 17*, 179-186.
35. Tarafdar, M., et al. (2014). The dark side of information technology. *MIT Sloan Management Review*.
36. 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.
37. Vance, A., et al. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. *Information & Management, 57*(4), 103212.
38. Von Solms, B. (2006). Information security–the fourth wave. *Computers & Security, 25*(3), 165-168.
39. 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
40. Xu, H., et al. (2019). Earnings management in firms with data security breaches. *Journal of Information Systems, 33*(3), 267-284.
41. Zeb, A., et al. (2021). The competing value framework model of organizational culture, innovation and performance. *Business process management journal*.