SINET: Ethiop. J. Sci., 46(3): 250-270, 2023 ISSN: 0379–2897 (PRINT)
 eISSN: 2520–7997

Date received: 10 June 2023; Date revised: 20 March 2024; Date accepted: 22 March 2024
DOI: https://dx.doi.org/10.4314/sinet.v46i3.3

The moderating impact of organizational culture on information security compliance

Kibrom Ejigu [1], Mikko Siponen [2] and Tilahun Muluneh [1]

[1] Addis Ababa University, Addis Ababa, Ethiopia. E-mail: kibromtadesse@gmail.com
[2] University of jyväskylä, Finland. E-mail: mikko.t.siponen@jyu.fi

ABSTRACT: This research paper investigates the association between organizational culture and employees' compliance with information security policies. Drawing upon rational choice theory (RCT) and the competing values framework (CVF), our study explores the moderating effects of cultural dimensions on information security compliance in a diverse range of organizations. We employ a scenario-based approach and analyze the data using Partial Least Squares Structural Equation Modeling (PLS-SEM). Our findings underscore the robustness of the model and emphasize the pivotal role of cultural dimensions in influencing employees' compliance intentions.

The study contributes by synthesizing non-fear-based deterrence theory with organizational culture theory, offering practical insights for information security managers. Recommendations include framing compliance as a moral duty, involving end-users in policy development, utilizing effective communication, implementing monitoring systems, and fostering a consistency culture. For organizations, the research underscores the importance of cultivating an ethical culture, emphasizing moral beliefs, and leveraging cultural dimensions to enhance compliance intentions.

Acknowledging limitations related to single-country data collection, a focus on compliance intentions, and the selection of organizations with established policies, this research paves the way for future studies. Future research should aim to replicate this study in diverse cultural settings, consider individual-level culture measurement, and explore additional moderating factors. This research contributes to understanding the intricate relationship between organizational culture and information security compliance, offering actionable insights for practitioners and prospects for further exploration in the information security field.

Keywords/ phrases: Information security, Information security policies, rational choice theory, competing values framework, organizational culture, Information security policies compliance

INTRODUCTION

Information security policies (ISPs) are crucial for safeguarding organizational data and assets, yet the persistent challenge of employee noncompliance with these policies remains a significant concern in various organizational settings(Vance, Siponen, & Straub, 2020). Because this issue is so important, previous research has helped us learn a lot about the factors that affect employees' refusal to follow rules(Karlsson, Karlsson, Åström, & Denk, 2022; Solomon & Brown, 2021; Vance et al., 2020). Past research in the field of information system security has made substantial progress by contributing to our knowledge of individual-related variables which expose employees' noncompliance(Herath & Rao, 2017; Vance, Siponen, & Pahnila, 2012; Vance & Siponen, 2012). Many studies have made great progress by using different theories from behavioural psychology and criminology to explain ISP compliance. For example, general deterrence theory and the theory of planned behaviour have been used(D'Arcy, Hovav, & Galletta, 2009; Sommestad & Hallberg, 2013). Also, researchers have looked into the idea of information security in organisational culture settings. This involves looking at what happens when people in a social group think, act, and value things in the same way (Karlsson et al., 2015).

Previous scholarly investigations have significantly enhanced our knowledge of the relationship between information securitiesand culture(Cram, D'arcy, & Proudfoot, 2019; D'Arcy & Greene, 2014; Van Niekerk & Von Solms, 2010). Moreover, these studies have shed light on the various factors that contribute to the development of information security(Hu, Dinev, Hart, & Cooke, 2012).Furthermore, studies have yielded valuable insights into factors that can enhance employees' compliance with information security policies (Bulgurcu, Cavusoglu, & Benbasat, 2010; Herath & Rao, 2009; Hu et al., 2012; Ifinedo, 2014; Siponen,

*Author to whom correspondence should be addressed.

Pahnila, & Mahmood, 2010; Sommestad, Hallberg, Lundholm, & Bengtsson, 2014)

Although past research demands recognition, it's important to highlight that Karlsson et al. (2015) noticed a relative lack of attention given to the effects associated with organizational cultures in the context of information security. This observation corresponds with our reviews of studies, suggesting that current research offers limited guidance to practitioners regarding the challenges associated with organizational cultures and their effects on employee compliance with ISPs. Additionally, a lot of empirical studies use the general deterrence theory (GDT) and/or protection motivation theory (PMT) which focus on fear-based strategies and give limited views (Vance and Siponen, 2012). Nevertheless, the rational choice theory (RCT) used in this study includes extra factors like expected benefits and moral beliefs, which gives a full picture of the problem of information security compliance (Li et al., 2010). Nevertheless, it is worth noting that a number of studies, such as Vance and Siponen (2012) and Li et al. (2010) have incorporated certain elements of the RCT framework in their investigations of ISP compliance. But, Cram et al. (2019) conducted a comprehensive literature review and observed that the majority of research in the context of ISP compliance has been carried out within developed countries, namely the People's Republic of China, Finland, the United States, and the Republic of Korea, while the distinct dynamics of developing nations have received limited attention(Tilahun & Tibebe, 2017). Therefore, further research is needed to determine the generalizability of the findings to diverse cultures. Hence, we present the research question: what is the effect of organizational culture on the employees' intention to comply with information security policies? This study investigates the moderating effect of organizational cultures on ISP compliance. By incorporating elements from Quinn and Rohrbaugh's (1983) theoretical framework of competing values and rational choice theory, this will be possible.

The rest of the paper is organized as follows: The current literature on employee compliance is explored briefly in the second section to demonstrate that most previous studies have examined ISP compliance and organizational culture. We then present the research model and respective research hypotheses. The fourth section describes the research method adopted for this study, followed by the results in the fifth section. In the final section, we discuss the implications for research and practice, along with the limitations of the study and directions for future research.

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, Proudfoot, & D'arcy, 2017). These policies depend on employee compliance for their effectiveness (Stafford, Deitz, & Li, 2018). Research shows that employees often violate these policies, driven by a perception of increased productivity(Tarafdar, D'arcy, Turel, & Gupta, 2014). This non-compliance poses challenges to an organization's efforts to maintain robust information security(Xu, Guo, Haislip, & Pinsker, 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 Van Muijen et al. (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 & 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. (2015), the aspects of organizational culture and information security policy compliance have been addressed to a very small degree in the current literature. However, the studies by Chang and Lin (2007), Donahue (2011), Hu et al. (2012), Solomon and Brown (2021), andKarlsson 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. Chang and Lin (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: consistency and effectiveness, examining how these orientations influence individuals' cognitive beliefs regarding information security policies. Solomon and Brown's (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, M., Karlsson, F., Åström, J., &Denk (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

Rational Choice Theory

We use RCT as the basis for our theoretical model, which explains individuals' decisions to engage in criminal behavior as a result of utilitarian calculations involving perceived benefits and formal and informal sanctions. RCT is widely applied to understand criminal behavior, as demonstrated by Vance and Siponen (2010), making it suitable for studying compliance with organizational IS security policies. Rational Choice Theory involves individuals carefully weighing the pros and cons before deciding whether to participate in criminal activities. According to Cao (2004) and Vance and Siponen (2010), it assumes that criminal behavior is intentional and rational. This behavior stems from evaluating the expected costs, sanctions, and benefits (Cao, 2004). In essence, individuals opt for criminal actions when the expected benefits outweigh the corresponding drawbacks.RCT is a well-accepted theory applied to various domains, including ISP compliance. Prior studies have employed different behavior theories, such as the theory of planned behavior (TPB) and protection motivation theory (PMT) but often provided limited insights due to their focus on fear-based strategies (Vance, Siponen et al. 2012). RCT offers a comprehensive perspective on information security by considering individual perceptions of compliance benefits or costs, informal and formal sanctions, and moral values. 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 examine various aspects of compliance behavior, including incentives (perceived benefits), disincentives (formal and informal sanctions), and the recent incorporation of moral beliefs into utilitarian calculations (Vance, 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, not all RCT constructs have been thoroughly studied in the African context (Tilahun and Tibebe 2017), and the concept of

shame has rarely been investigated concerning employees' ISP compliance. 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. The concept of shame within the framework of RCT remains underrepresented in research, offering an opportunity for further investigation, especially in diverse cultural and socioeconomic contexts. There aren't many studies that look at all RCT constructs in low-income countries, especially in Africa. This makes people wonder if existing compliance models can work in places with different cultural and economic factors.

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 & Lin, 2007; Hu et al., 2012; Karlsson et al., 2022; Solomon & 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, Siponen, Puhakainen, & Sarker, 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, De Vries, & Comiskey, 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.

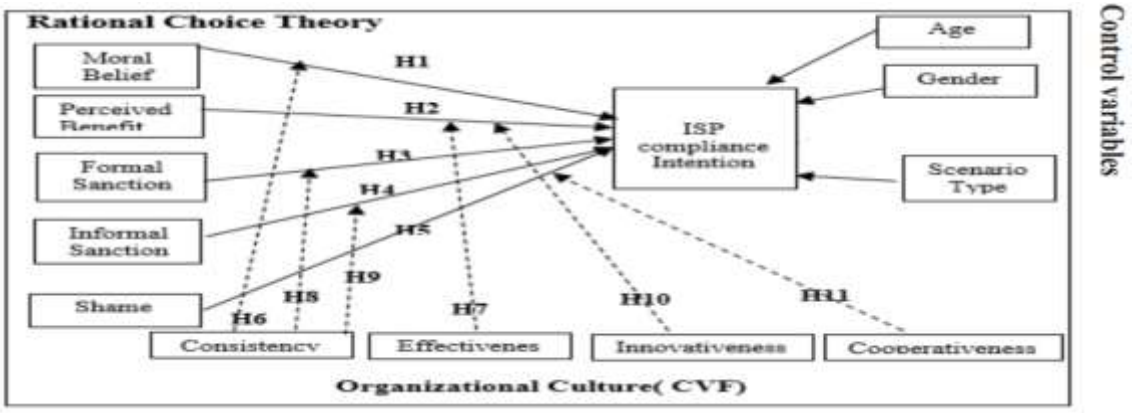

Figure 1: Research Model

Hypotheses

Moral belief

Moral beliefs reflect people's judgments about what is morally right or wrong and profoundly influence their behavior and intentionsA., Siponen, M. T., & Straub, D. W. (2020). In the context of information security policy compliance, moral beliefs pertain to an employee's perception of compliance with organizational policies as morally acceptable. Strong moral beliefs regarding policy compliance correlate with a higher likelihood of adherence. Extensive research supports the significant impact of moral beliefs on compliance intentions with information security policies. For instance, Vance and Siponen (2012) found moral beliefs to be the most influential factor in compliance intention with ISPs in their RCT-based model. Similarly, Li et al. (2010) demonstrated the positive effect of moral beliefs on compliance intention with internet policies within an RCT-based model. Myyry et al. (2009) also noted that individuals' values and moral reasoning can predict information security policy compliance.Moreover, Vance, Siponen, and

Straub (2020) suggested that the rule-breaking behavior is contingent on an individual's moral beliefs. Individuals with strong moral beliefs view rule-breaking as morally wrong. In contrast, individuals with weaker moral beliefs may not see rule-breaking as morally wrong. This indicates that moral beliefs hold substantial sway over decisions involving deviant and criminal behaviors. Individuals who perceive noncompliance with the ISP as morally wrong are less likely to violate information security policiesVance, Siponen, and Straub (2020). Based on previous research on moral beliefs, we hypothesize that moral beliefs could influence ISP compliance intention, as follows:
H1: Moral beliefs positively influence employees' intentions regarding ISP compliance.

Perceived Benefits

Perceived benefits, rooted in rational decision-making, involve evaluating available choices to select the one offering greater satisfaction or perceived advantages(Pogarsky, 2009). Studies based on RCT have consistently found that perceived benefits serve as reliable predictors of ISP compliance(Sommestad et al., 2014). This relationship implies that compliance is positively associated with individuals perceiving personal benefits from adhering to organizational policies(Tyler & Blader, 2005). Empirical research based on RCT suggests that individuals contemplating deviant or illicit acts assess the perceived benefits of such behavior. A higher likelihood of deviance occurs when the benefits outweigh the costs, and the potential for detection and punishment is low(Moody, Siponen, & Pahnila, 2018). In the context of information security, perceived benefits significantly determine compliance behavior(Ifinedo, 2016). Siponen and Vance (2012) have reported a substantial positive effect of perceived benefits on employees' ISP behavioral intention. Consequently, it can be argued that ISP compliance intentions are shaped by an individual's perception that compliance will yield personal benefits (Bulgurcu et al., 2010). Generally, perceived benefits are a critical factor in employees' compliance decision-making processes, driving their intentions to adhere to information security policies in organizational settings.Hence, the hypothesis can be posited that perceived benefits have a significant positive effect on employees' complainsintentions with information security policies.Therefore, we hypothesize the following:
H2: Perceived benefit of compliance is positively related to employees' intention towards ISP compliance.

Formal and Informal Sanctions

Formal sanctions, explicit punishments for specific acts of misconduct, play a crucial role in the context of deterrence theory within ISP compliance. According to Ifinedo (2016), the RCT asserts that individuals engage in decision-making processes by conducting a thorough evaluation of the potential benefits and costs associated with their choices.Formal sanctions increase compliance, by motivating employees to adhere to ISPs.Studies on the relationship between formal sanctions and ISP compliance show that warnings and penalties significantly boost employees' adherence(Tang, Li, & Zhang, 2016).Maignan and Ferreira (2019) also found thatthe threat of formal sanctions predicts employee compliance. D'Arcy et al. (2009) found that sanction affects users' intentions to commit computer abuses, while Aurigemma and Mattson (2014) identified its impact on employees' ISP compliance intent. Punishment had mixed effects(Herath & Rao, 2017).According to A., Siponen, M. T., & Straub, D. W. (2020) neither formal nor informal sanctions effectively explain employees' intention to comply with the ISP.The inconsistent results warrant further empirical investigation(Ifinedo, 2016; Johnston, Warkentin, McBride, & Carter, 2016; Roberts, 2021) . These contradictory results inspire the present investigation into ISP compliance and the cultural analysis of formal sanction and informal sanction within organisations.

Informal sanctions, unspoken rules governing behaviour within an organization, significantly impact ISP compliance intentions. Social control theory suggests individuals conform due to the fear of social sanctions(Siponen et al., 2010). Informal sanctions like peer pressure, social disapproval, and the risk of losing trust motivate adherence to ISP.Empirical evidence supports this. Niu and Guo (2019) found that informal sanctions positively influence compliance intentions. Liu, Ma, and Zhang (2020) reported positive effects of perceived social pressure.Yu and Lu (2016) demonstrated that informal sanctions are more effective in promoting information security compliance than technical controls. Studies attest to the impact of informal sanctions in reducing non-compliance(K. Ejigu, Siponen, & Muluneh, 2021; Kaviani, Young, Robards, & Koppel, 2020).Informed by theory and empirical evidence, it can be postulated that formal and informal sanctions significantly and positively affect information security policy compliance intentions. Incorporating formal and informal

sanctions can effectively promote compliance among employees, emphasizing their importance for organizations.Consequently, we integrate the impacts of both formal sanctions and informal sanctions into our model in the following manner:

H3: Formal sanctions positively relate to employees' ISP compliance intentions.

H4: Informal sanctions positively relate to employees' ISP compliance intentions.

Shame

Shame has been examined in the literature as a potential influencer of employees' intentions towards complying with information security policies. Shame can serve as a powerful motivator for behavior change, especially when an individual's reputation is at risk(Willison & Warkentin, 2013). It can lead to a heightened sense of responsibility and accountability(Vance et al., 2020). In this context, individuals who experience shame in response to potential noncompliance with an ISP may perceive the policy as more important and feel more motivated to comply(Vance et al., 2020). This aligns with previous studies that associate shame with increased moral awareness and sensitivity(Tangney & Dearing, 2002).Social pressure stemming from shame can also influence compliance. Those concerned about their reputation may be more inclined to adhere to ISP to avoid negative social consequences, such as ridicule or ostracism (Vance et al., 2020). This is consistent with earlier research indicating that social pressure is effective in promoting compliance with organizational policies and regulations (Gino & Pierce, 2010).Empirical studies support the positive effect of shame on ISP compliance intentions. For example, Vance et al. (2013) found that shame was a significant predictor of compliance intention among employees in a healthcare organization. Similarly, Ifinedo and Nahar (2014) found that shame predicted compliance intention among employees in a Canadian university.When employees experience shame, they are less likely to intend to violate information security policies. In this case, the negative impact of shame is associated with a reduced intention to violate policies, which indirectly implies a higher intention to comply with those policies(Vance et al., 2020). We hypothesize, based on prior research on shame, that shame may affect information security behavior.

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

Consistency culture

Consistency culture, characterized by a strong emphasis on control and strict compliance behavior, is often described as a controlling, rule-oriented, or hierarchical culture. It prioritizes order, efficiency, and uniformity, featuring a well-defined organizational structure, standardized policies and rules, and clear responsibilities(Ernest Chang & Lin, 2007). Moral belief depends upon the belief that individual' perceptions of what is morally right and wrong have a significant influence on their intentions and subsequent actionsVance et al.,(2020).Moral beliefs play a critical role in influencing employee behavior, particularly in the context of ISP compliance(Siponen et al., 2010). When employees perceive alignment between their moral values and their organization's actions, they are motivated to comply with policies. In contrast, when there is adisconnect between their moral values and their company's actions, it can undermine their motivation to comply with policies (Tyler & Blader, 2005). The alignment between moral beliefs and organizational rules and values significantly influences individual behaviors(Carlsmith, Darley, & Robinson, 2002). Hence, we argue that in a consistency culture, the alignment between moral beliefs and compliance intentions is strengthened because, the culture's emphasis on strict rule adherence, hierarchy, and control fosters an environment where employees not only view compliance as a rule-based requirement but also as a morally justifiable action. As employees assess the morality of organizational policies and practices, consistency culture's alignment with moral beliefs encourages ISP compliance intentions.Studies suggest that ethical values significantly shape behavior when employees believe that organizational rules and values are consistent with their moral beliefs(Di Stefano, Scrima, & Parry, 2019). This alignment between morality, rules, and values is particularly relevant in the context of ISP compliance, where decisions involve moral elements(Vance et al., 2020). Therefore we argue that consistency culture enhances the positive effect between moral beliefs and ISP compliance intention. The strict adherence to rules and the alignment of organizational values with moral beliefs create a conducive organizational environment that strengthens the motivation for ISP compliance based on moral considerations. Therefore, we propose a hypothesis that:

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

Effectiveness

Chang and Lin (2007) defined effectiveness culture as one emphasizing competition, goal achievement, benefit orientation, and productivity measures. It is often referred to as the market culture, characterized by intense competition among employees. In this culture, assertiveness, competition, and a focus on material incentives are encouraged, and benefit-oriented leadership prevails. Individuals often find themselves competing for career development, advantages, and resources, and this culture is conceptually linked to a norm of competition (Di Stefano et al., 2019). Yukl (2002) suggests that increased productivity and intense competition for rewards and promotions in organizations can lead to more frequent unethical behavior. Similarly, perceived benefits is defined as a rational decision-making process where individuals assess available choices and analyze the outcomes of each option to select the one that offers greater satisfaction or perceived benefits(Siponen et al., 2010).

Here, we argue that in the context of an effectiveness culture, where individuals are motivated by the pursuit of career development, advantages, and resources through competition, the perception of benefits gained from compliance with ISPs becomes a crucial factor influencing their intentions. Perceived benefits play a significant role in shaping employees' compliance intentions in organizations with an effectiveness culture, where individuals compete to achieve organizational objectives and where rewards and promotions may further influence their intention to comply with ISPs.Therefore, the relationship between perceived benefits and effectiveness culture is one where the competitive and benefit-oriented nature of an effectiveness culture aligns with rational decision-making driven by the perceived advantages of compliance. This alignment strengthens the positive effect of perceived benefits on compliance intentions, which is hypothesized in

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

Consistency culture

Formal sanctions, characterized by explicit punishments for misconduct, are recognized as a cornerstone of deterrence theory, motivating individuals to adhere to ISPs. The RCT asserts that people weigh potential benefits against potential costs in decision-making. In this context, formal sanctions increase compliance by introducing a cost factor for non-compliance. The existing body of research highlights that formal sanctions significantly enhance adherence to ISPs (K. T. Ejigu, Siponen, & Arage, 2021), even the mere threat of formal sanctions predicts compliance (Maignan and Ferreira, 2019).Consistency culture, marked by a strict commitment to rules and procedures(Di Stefano et al., 2019; Ernest Chang & Lin, 2007), aligns seamlessly with the enforcement of formal sanctions. Here, we argue that the culture's emphasis on rule adherence, hierarchy, and standardized policies creates an environment in which employees are more likely to respond to the explicit consequences of non-compliance. The strict organizational structure and rule-oriented approach of a consistency culture reinforce the link between formal sanctions and compliance intentions, making it a pivotal factor within this context.

Informal sanctions, encompassing unspoken rules and social pressures, significantly impact ISP compliance intentions(Siponen et al., 2010; Vance & Siponen, 2012). Social control theory suggests that individuals conform due to the fear of social sanctions.Here, we also argue thatin a consistency culture, the effectiveness of informal sanctions is further amplified. The culture's strict adherence to standardized rules and procedures creates an environment where peer pressure, social disapproval, and trust considerations are more likely to influence employees' compliance intentions. The dominance of rule-based procedures in a consistency culture ensures that employees are more likely to respond to both formal and informal consequences for non-compliance, thus reinforcing the influence of informal sanctions.A consistency culture creates synergy between formal and informal sanctions. It fosters an environment where both types of sanctions can work in tandem to promote compliance intentions. The culture's focus on rule adherence ensures that employees are more likely to respond to both formal consequences and social pressures, making it a powerful combination for encouraging compliance with ISP.Hence, we propose the following hypotheses:

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

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

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 & 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, Siponen, & Muluneh, 2021).

In ISP compliance studies, perceived benefits have been found to positively affect compliance intention (Siponen et al., 2010) . We argue that the effect of perceived benefits on compliance intention may be moderated by the organizational culture value of innovativeness. In other words,in an innovative culture, employees are encouraged to take risks and try new approaches to problem-solving. Perceived benefits of ISP compliance, such as improved efficiency and effectiveness, may align well with the values of innovation and experimentation. Therefore, employees may be more willing to comply with ISP policies if they perceive that doing so will contribute to the innovative culture of the organization. Similarly, 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) and Bassett (2007), 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 innovativeness culture, perceived benefits and ISP compliance intention. The findings by Karlsson et al (2022) raise questions about the conditions under which such cultures may have divergent effects. Therefore, we propose that an innovative culture strengthens the positive effect between perceived benefits and ISP compliance intentiondue 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:

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

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 culture emphasizes cooperation, group rewards, and discourages violations of group norms, values, and beliefs and is characterized by a sense of belonging and loyalty to the organization(Di Stefano et al., 2019; Ernest Chang & Lin, 2007). Employees are encouraged to share information and collaborate to achieve organizational goals, with group rewards taking precedence over individual contributions. As a result, breaches of group norms and values are strongly discouraged, and employees prioritize the group's interests(Di Stefano et al., 2019). Shame, akin to sanctions, may deter individuals from engaging in unlawful activities(Vance & Siponen, 2012; Vance et al., 2020). Studies have shown that a cooperativeness culture values cooperation and group rewards over individual contributions, with employees acting in the interest of the group and discouraging harmful behaviors(Di Stefano et al., 2019). Breaching group norms and beliefs in such a culture triggers shame(Di Stefano et al., 2019), discouraging individuals from engaging in illicit activities (D'arcy & Herath, 2011). Shame is closely tied to the concept of group influence and norms(Tadesse et al., 2021). Prior research has suggested that shame has a negative impact on ISP violations within an organization (Siponen & Vance, 2010; Vance et al., 2020). Experiencing shame is more likely to conform to group norms and less likely to engage in non-compliant behavior social disapproval, or shame, effectively deters people from unlawful activities, as evidenced by Siponen et al. (2010). Therefore, if non-compliance with ISPs is seen as a breach of group norms, we can argue that shame has a substantial influence on ISP compliance within a cooperativeness culture(D'arcy & Herath, 2011; Di Stefano et al., 2019; Siponen et al., 2010). Here we also argue that in a cooperativeness culture, employees prioritize the group's interests over their individual goals. If ISP compliance aligns with a group norm, individuals within such a culture are more likely to adhere to these norms, potentially strengthening or dampening the effect of shame on their compliance intention. This underscores the pivotal role that cooperativeness culture plays in shaping

compliance intentions and highlights the close alignment between the emotional response of shame and the cultural norms and values of cooperativeness. Therefore, we hypothesize that:
H11: Cooperativeness culture amplifies the positive effect of shame on compliance intention.

Method

We employed a scenario-based method, to investigate employee information security policies compliance. This method presents participants with fictional scenarios, followed by questions about their likelihood of behaving similarly in analogous situations(Vance et al., 2020). This approach aligns with RCT, which involves individuals evaluating the costs and benefits of illegal behavior, making it well-suited for RCT studies. The scenario method offers detailed descriptions of specific violations, enabling participants to make instinctive decisions regarding ISPs compliance. Furthermore, it offers a less confrontational approach to assessing intentions compared to direct self-reports(Vance & Siponen, 2012; Vance et al., 2020). Our scenario design involved collaboration between the company's information security officers and the research team. Based on the research work of(Siponen et al., 2010; Vance & Siponen, 2012), we used a belief-elicitation technique to conduct a survey of 108 IT information security officers.We collected responses from 54 practitioners, resulting in a 50% response rate. We categorized and ranked the top five information security policy compliance concerns identified by the officers: password sharing, failure to log out from workstations, sharing customer information, using USB drives, and not reporting computer virus incidents.

To ensure the reliability and validity of our instrument, we conducted both a pre-test and a pilot test. A pre-test involved 66 experts from Ethiopia and Finland, including practitioners and academicians, providing feedback. We made adjustments to the survey instrument based on their input, including simplifying language, improving question flow, and item wording. The pilot test involved around 100 employees, with 61 completing the questionnaire (17% response rate). The analysis confirmed the instrument's validity and reliability, with Cronbach's α value above .84.In our primary data collection phase, we systematically selected a representative sample from key Ethiopian cities for studying information security policy compliance. We faced challenges in creating a comprehensive list of organizations with information security policies due to limited documentation. To address this, we strategically selected cities with known ISPs, employing random sampling to approach staff members in these organizations. We engaged experts familiar with Ethiopian demographics and culture to include employees from diverse regions. We identified five representative cities: Adama,Addis Ababa, Bahir Dar, Dire Dawa, Hawassa, and Mekele.

For our sample, we identified organizations known for well-established information security policies through interactions with ministerial offices at regional and federal levels. We received a list of approximately 700 organizations, from which we employed random sampling to select representative organizations. These included banks, insurance companies, universities, city administrations, and Ethiotelecom offices. The organizations provided lists of employee names, from which we randomly selected respondents. We used paper-based surveys due to internet connectivity challenges. We collected 553 usable responses, resulting in a 21% response rate, exceeding the minimum threshold for meaningful analysis.Our primary data collection process included strategic city and organization selection, random respondent sampling, and meticulous survey distribution and collection, ensuring a representative sample and a substantial dataset for our study on information security policy compliance in Ethiopia.

RESULTS

This study utilized PLS-SEM due to its ability to assess measurement and structural models concurrently and its applicability for empirical theory-building research. 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.

Measurement Model Evaluation

The assessment of the measurement model in Partial Least Squares (PLS) analysis is an essential step in maintaining the model's reliability and validity. This evaluation focuses on four critical elements, as suggested by Hair et al. (2017) and Sarstedt et al. (2019): indicator reliability, internal consistency reliability, convergent validity, and discriminant validity. A visual representation of the measurement model is presented in Figure 4.1.

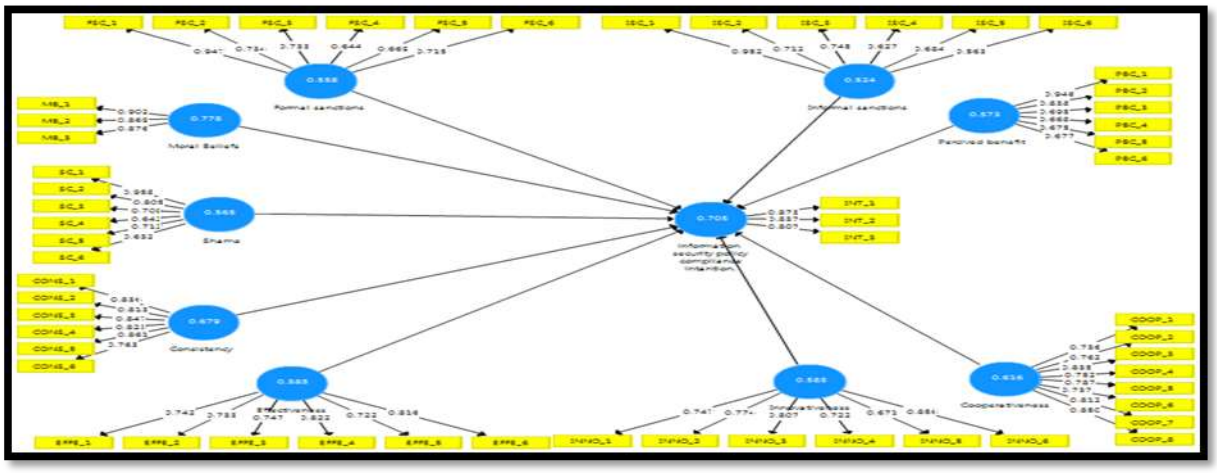

Figure 2: Measurement mode

Measurement reliability was assessed through indicator reliability, Cronbach's alpha (α), correlation, and composite reliability. All ten constructs demonstrated outer loadings exceeding 0.60, surpassing the 0.50 acceptability threshold suggested by Chin (1998), as depicted in Figure 2 and Table 1. For Cronbach's alpha (α) and composite reliability (CR), in line with Hair Jr et al.'s (2017) guidelines, the results in Table 1 indicate that all composite reliability values, ranging from 0.870 to 0.928, exceed the specified threshold of > 0.70. Furthermore, the Cronbach's Alpha values, exceeding 0.7, align with Sekaran's (2006) criteria. The average variance extracted (AVE) values for all constructs were also above the recommended threshold of 0.50 (Hair, 2017).

Table 1.

Latent Variables		Factor loading	α >0.70	CR >0.70	AVE >0.50
1.	Shame	0.632-0.958	0.913	0.913	0.778
2.	Consistency	0.763-0.836	0.893	0.888	0.573
3.	Cooperativeness	0.736-0.850	0.887	0.881	0.558
4.	Effectiveness	0.742-0.816	0.870	0.865	0.524
5.	Formal sanctions	0.715-0.947	0.889	0.884	0.565
6.	Informal sanctions	0.563-0.952	0.927	0.927	0.679
7.	Innovativeness	0.747-0.856	0.895	0.894	0.585
8.	Moral Beliefs	0.876-0.902	0.897	0.894	0.585
9.	Perceived benefit	0.677- 0.946	0.928	0.928	0.616
10.	Intention	0.807-0.873	0.877	0.877	0.705

The results indicate the model's suitability for further structural equation modeling. All latent variables exhibit factor loadings exceeding 0.70, signifying robust relationships between observed variables and their respective latent constructs. Moreover, both Cronbach's alpha (α) and composite reliability (CR) values surpass 0.70, demonstrating strong internal consistency and reliability among the latent variables. AVE values also exceed the recommended threshold of 0.50, affirming that latent variables account for a substantial amount of variance in their respective indicators. These findings robustly support the model's reliability for investigating the research's relationships and hypotheses. Discriminant validity was assessed through well-established methods, including cross-loadings, the Larcker criterion (square root of AVEs), and the novel heterotrait-monotrait ratio of correlations (HTMT).

Table 2: Discriminant validity assessment using the Fornel–Larckert criteria

Latent variables		1	2	3	4	5	6	7	8	9	10
1.	Shame	0.751									
2.	Consistency	0.256	0.824								
3.	Cooperativeness	-0.031	0.440	0.785							
4.	Effectiveness	0.025	0.514	0.382	0.765						
5.	Formal sanctions	0.732	0.147	-0.112	-0.003	0.747					
6.	Informal sanctions	0.624	0.187	-0.033	0.055	0.721	0.724				
7.	Innovativeness	0.001	0.256	0.344	0.224	-0.005	0.119	0.765			

Table 2 reveals that none of the correlations equaled or exceeded the square root of the AVE, providing strong evidence of discriminant validity. The analysis adheres to the Fornel-Larcker criteria, confirming that the model's measurements satisfy the criterion of discriminant validity. Furthermore, indicators do not exhibit higher loadings on opposing constructs, affirming ample discriminant validity among all constructs (Hair et al., 2011).The HTMT an innovative approach for evaluating discriminant validity in SEM, was employed in this study, aligning with Henseler et al.'s (2015) recommendation. Table 3 illustrates that all HTMT ratios for each construct are below 0.9, confirming the satisfactory establishment of discriminant validity.

Table 3: HTMT ratios

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	

Results of the structural model

We utilized a rigorous PLS bootstrapping resampling method, employing 5000 subsamples, while adhering to the default settings (i.e., parallel processing without sign changes). This approach was employed to assess the path coefficients and determine their levels of statistical significance (Streukens & Leroi-Werelds, 2016).

The results are summarized in Table 4.11, which indicates VIF values comfortably below the recommended threshold of 5.0, ranging from 1.306 to 3.622, affirming the structural model's robustness and ruling out concerns about multicollinearity(Hair, 2017).The R^2 value for information security policy compliance intention, presented in Table 4.11, was calculated at 0.813. This substantial R^2 value, following Cohen's (1998) guidelines, indicates that 81.3 percent of the variance in information security policy compliance intention is explicable by the independent variables.The results, detailed in Table 4.11, revealed a positive Q^2 value of 0.530 for information security policy compliance intention. This positive value signifies the model's predictive relevance for this crucial factor, aligning with established standards (Latan, Noonan, & Matthews, 2017). Finally, effect size (f^2) was evaluated to assess the practical significance of relationships within the structural model. As per Cohen's (1998) criteria, the effect sizes for moral beliefs, perceived benefit, formal sanctions, informal sanctions, and shame on employees' intention toward ISP compliance, as shown in Table 4.12, all fall within the small effect size category.

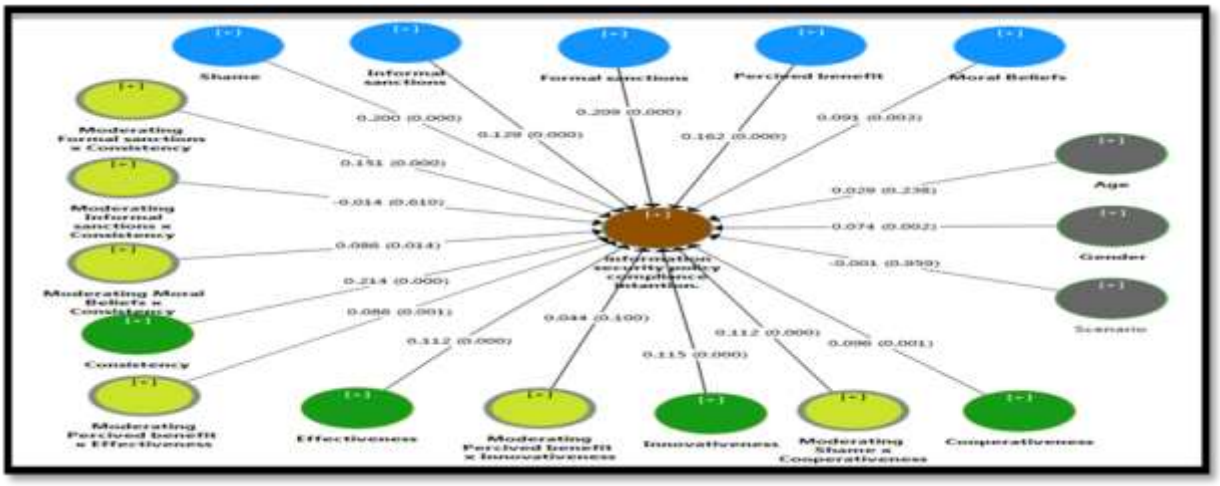

Figure 3: Structural Model

Direct Effects

This section provides critical insights into the relationships between key constructs through the evaluation of direct effects within the structural model. Table 4 offers a summary of path coefficients, t-statistics, p-values, VIF, and f^2 effect sizes for each hypothesis. The control variables analysis reveals that gender significantly influences intention, whereas age and scenario types do not exhibit statistically significant effects on compliance intention in this study. This underscores the relevance of gender as a control variable when exploring compliance intention within the context of information policy.Our first hypothesis (H1) postulated a positive relationship between moral beliefs and employees' intentions toward ISP compliance. As depicted in Table 4, the path coefficient (β) is 0.091, with a t-value of 2.977 and a p-value of 0.003. These statistical results support H1, with a p-value below 0.05, signifying statistical significance. This affirms that moral beliefs positively influence employees' intentions toward ISP compliance. The standardized estimate reinforces this relationship (H1: $\beta = 0.091$; t-value = 2.977; $p < 0.01$).

Hypothesis 2 (H2) proposed a positive relationship between the perceived benefit and employees' intentions toward ISP compliance. The results in Table 4 reveal a path coefficient (β) of 0.162, a t-value of 4.296, 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 perceived benefit of compliance indeed exerts a positive influence on employees' intentions toward ISP compliance.Our third hypothesis, H3, suggested a positive relationship between formal sanctions and employees' intentions toward ISP compliance. Table 4 presents a path coefficient (β) of 0.209, a t-value of 4.826, and a p-value of 0.001, all indicating robust statistical support for H3. This confirms that formal sanctions have a substantial positive impact on employees' intentions toward ISP compliance.

Hypothesis H4 postulated a positive relationship between informal sanctions and employees' intentions toward ISP compliance. The statistical analysis, as shown in Table 4, yields a path coefficient (β) of 0.129, a t-value of 3.837, and a p-value of 0.001. These results provide strong support for H4, with a highly significant p-value. Thus, it is evident that informal sanctions exert a positive influence on employees' intentions toward ISP compliance.The final hypothesis, H5, proposed a positive relationship between shame and employees' intentions toward ISP compliance. The analysis in Table 4 demonstrates a path coefficient (β) of 0.200, a t-value of 4.223, and a p-value of 0.001. These results firmly support H5, with a p-value well below the significance threshold. Therefore, the findings confirm a positive association between shame and employees' intentions toward ISP compliance.

Effect sizes (f^2) provide insights into the practical significance of the relationships under investigation. As a rule of thumb, values greater than 0.02, 0.15, and 0.35 indicate small, medium, and large effect sizes, respectively (Cohen, 1998). As shown in Table 5, the f^2 effect sizes for moral beliefs (H1), perceived benefit (H2), formal sanctions (H3), informal sanctions (H4), and shame (H5) on employees' intention toward ISP compliance are all categorized as small. This suggests that while these relationships are statistically significant, their practical impact may be relatively modest.In conclusion, the assessment of direct effects within the structural model affirms the validity of our hypotheses, highlighting the positive relationships between moral beliefs, perceived benefit, formal sanctions, informal sanctions, shame, and employees' intention toward ISP compliance.

Additionally, the effect size analysis underscores the practical significance of these relationships, categorizing them as small but meaningful within the context of the study.

Table 4. Structural model estimates.

Latent variables	VIF	Endogenous constructs	R^2	Q^2
Moral Beliefs	1.423	**ISP compliance intention**	**0.813**	**0.530**
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			

**Not hypothesized paths*

Table 5 Structural model estimates and result of direct and moderation (interaction) effect.

Direct Effect Path	Beta	T Statistics	P Values	f2	Results
Moral Beliefs -> ISP compliance intention	0.091	2.977	0.003	0.041	Accept
Perceived benefit -> ISP compliance intention	0.162	4.296	0.001	0.059	Accept
Formal sanctions -> ISP compliance intention	0.209	4.826	0.001	0.080	Accept
Informal sanctions -> ISP compliance intention	0.129	3.837	0.001	0.042	Accept
Shame -> ISP compliance intention	0.200	4.223	0.001	0.076	Accept
Moderation (interaction) path					
Moral Beliefs x Consistency -> ISP compliance intention	0.086	2.446	0.014		Accept
Perceived benefit x Effectiveness -> ISP compliance intention	0.086	3.359	0.001		Accept
Formal sanctions x Consistency -> ISP compliance intention	0.151	4.454	0.001		Accept
Informal sanctions x Consistency -> ISP compliance intention	-0.014	0.510	0.610		Reject
Perceived benefit x Innovativeness -> ISP compliance intention	0.044	1.646	0.100		Reject
Shame x Cooperativeness -> ISP compliance 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

Moderation (Interaction) Effect

Analyzing moderation effects within the structural model sheds light on the intricate interplay between cultural factors and the relationships among key constructs. Table 5 provides a comprehensive overview of the moderation analysis, encompassing path coefficients, t-statistics, p-values, and their implications.

Our initial hypothesis (H6) posited that the presence of a consistency culture strengthens the positive influence of moral beliefs on individuals' compliance intentions. The results presented in Table 5 offer empirical support for H6, demonstrating a statistically significant moderating effect (H6: β= 0.086; t-value= 2.446; p< 0.05). Additionally, Figure 4 visually represents this interaction with three distinct lines illustrating the relationship between moral beliefs (x-axis) and ISP compliance intention (y-axis).

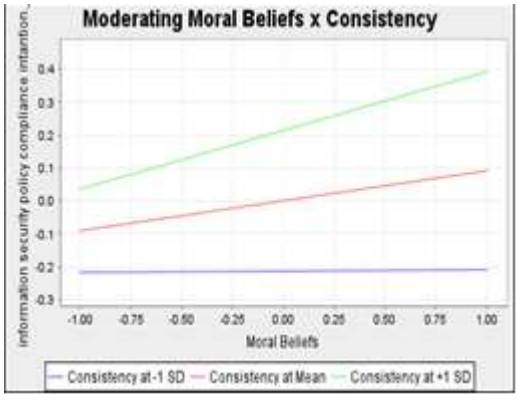

Figure 4. The interaction effect of moral beliefs x consistency on ISP compliance intention.

The middle line signifies the correlation within an organization characterized by an average-level consistency culture. The remaining two lines depict this association in scenarios with 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. It's evident that all three lines display apositive slope, indicating a positive correlation between moral beliefs and compliance intention. The findings suggest that the positive association between moral beliefs and compliance intention is stronger when consistency culture is high, while it becomes relatively weaker in organizations with low consistency culture. This discovery underscores the importance of a consistency culture in amplifying the impact of moral beliefs on compliance intentions.

Hypothesis H7 posits that the presence of an effectiveness culture strengthens the positive relationship between perceived benefits and compliance intention. This hypothesis is supported by statistically significant results, as presented in Table 5, which demonstrate a significant moderating effect of effectiveness culture on the association between perceived benefits and compliance intention (H7: β= 0.086, t =3.359, P < 0.001).

To provide further clarity on this correlation, Figure 5 displays three separate lines depicting the relationship between different levels of effectiveness culture. The central line in Figure 5 illustrates the correlation between perceived benefits and compliance intention when effectiveness culture is at a moderate level. Importantly, the observed trend in this line shows a positive incline, indicating that an increase in perceived benefits is associated with a greater inclination to comply, even when considering the average level of effectiveness culture. However, the significance of Hypothesis H7 becomes more pronounced when considering the lines representing elevated and diminished levels of effectiveness culture. At higher levels of effectiveness culture, there is a noticeable amplification in the influence of perceived benefits on compliance intention.

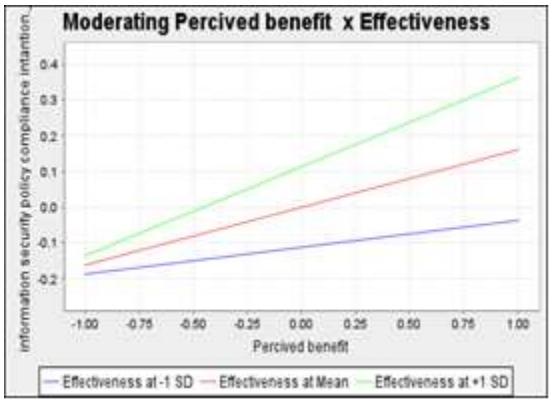

Figure 5: The interaction effect of perceived benefit x effectiveness on ISP compliance intention

Hypothesis H8, proposing that consistency culture moderates the relationship between formal sanctions and compliance intention, receives substantial support from the empirical data presented in Table 4.15, where the moderating effect of consistency culture is statistically significant (H8: β= 0.151, t-value = 4.454, P < 0.001).

To provide a visual representation of this interaction, Figure 6 illustrates three distinct lines, each representing the relationship between formal sanctions (x-axis) and compliance intention (y-axis). The middle line corresponds to organizations with an average level of consistency culture. Nearby the middle line are two additional lines, symbolizing scenarios with 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 of this cultural variable. 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 intention among employees.

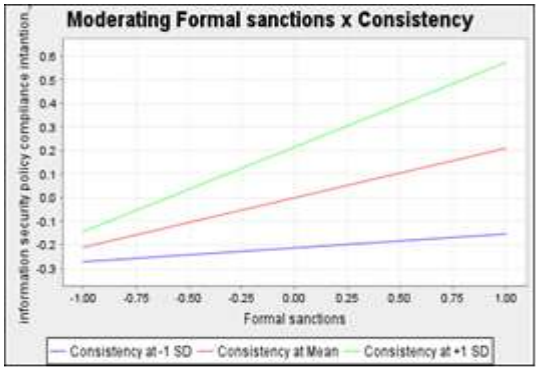

Figure 6: The interaction effect of formal sanction x consistency on ISP compliance intention

According to the findings presented in Table 5, 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 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.

The empirical analysis, as presented in Table 5, provides support for H11, (H11: β = 0.112, t-value = 4.535, P < 0.001) indicating that cooperativeness culture indeed plays a significant role in enhancing the positive relationship between shame and compliance intention. Figure 7 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).From the graphical representation, 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.

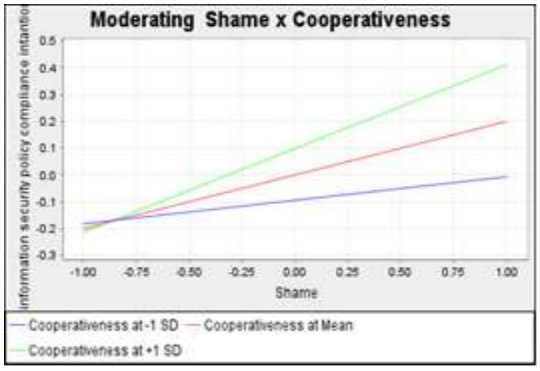

Figure 7: The interaction effect of shame x cooperativeness on ISP compliance intention

DISCUSSION

The support for Hypothesis H1 is well-founded and substantiated through statistical evidence and alignment with established theories across disciplines. According to Becker's 1968 introduction of the rational choice theory, people tend to make decisions that are in line with societal norms and values when they are strongly morally motivated. The connection between moral beliefs and employees' intent to comply withISPs is both statistically significant and conceptually consistent with findings in criminology, psychology, and ISS literature. Research in criminology has linked lower moral convictions with corporate crime and tax evasion(Paternoster & Simpson, 1996), (Wenzel, 2004). In psychology, studies have indicated that robust moral reasoning contributes to positive behaviors(Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009). Importantly, the existing literature on information security consistently shows that moral beliefs significantly influence employees' intent to comply. Studies like Li et al. (2010), Siponen and Vance (2012), D'Arcy et al. (2009), and Siponen (2000, 2002) show that moral beliefs play a big part in how likely people are to follow the rules. Consequently, this acceptance underscores the critical role of moral convictions in enhancing information security practices within organizations.

Large amounts of statistical evidence support the validity of Hypothesis H2, and it fits with well-known theories like rational choice theory. RCT suggests that individuals make choices by assessing outcomes and perceived benefits, selecting options promising greater satisfaction or perceived benefits. Empirical research in criminology and information security also consistently shows that how employees see the benefits of following compliance rules has a big effect on how likely they are to follow information security policies (ISPs). RCT, which contends that people make decisions based on perceived benefits, further strengthens the theoretical support for H2. Research by Ducan et al., (2005) and empirical studies in information security align with this notion. For instance, Vance and Siponen (2012) found that employees who perceived benefits from complying with information security policies were more likely to express positive intentions. In contrast, Li et al. (2010) reported a significant negative influence of perceived benefits on employees' compliance intentions with the policy. It is important to note, though, that Hypothesis H2 is only about ISP compliance and says that there is a positive relationship between employees' perceived benefits and their intention to comply with ISP rules. This may be different from what we see when we look at internet use policy compliance.

Acceptance of Hypothesis H3 shows how important formal punishments are as a strong deterrent in getting employees to follow information security policies. Formal sanctions, which encompass explicit penalties for specific misconduct, are central to deterrence theory an extension of rational choice theory. According to RCT, formal sanctions effectively deter undesirable behaviors. This theoretical premise is supported by real-world examples, such as Straub's (1990) study on computer abuse, which found that users were less likely to do wrong when they knew they would be punished for it.

Additionally, D'Arcy et al. (2009) demonstrated the substantial influence of formal sanctions on users' intentions concerning computer abuses. Hu, et al. (2010) research also revealed a significant relationship between formal sanctions and their impact on employees' intentions regarding computer offenses. Additionally, as Paternoster and Simpson (1996) and Pratt et al. (2006) demonstrate, our study is consistent with criminological research. The acceptance of Hypothesis H3 is based on strong theoretical principles and strong empirical evidence. This shows how important formal sanctions are in shaping ISPs' intentions to follow the rules. These findings contribute to a deeper understanding of the relationship between ISP compliance and formal sanctions across diverse organizational contexts.

The landscape of previous research into ISP compliance behavior presents a varied and mixed picture. Numerous studies, including those by Johnston (2015), Ifinedo (2014), and Xiaofeng (2016), have explored this field, yielding diverse outcomes. According to some studies, Ifinedo(2016)'s demonstration shows that informal sanctions' reliability in promoting ISP compliance is not always reliable. In contrast, Vance et al., (2020) reported a lack of a direct impact of informal sanctions on ISP compliance. These findings have contributed to a nuanced understanding of the role of informal sanctions within the context of ISP compliance. However, it is essential to emphasize that the research landscape is not uniform in its conclusions. Certain studies, such as those by Barlow (2017) and Moody et al. (2018), have presented evidence that informal sanctions can indeed exert a significant influence on compliance and effectively encourage ISP compliance behavior. These different results show how complicated the link is between informal sanctions and ISP compliance. They suggest that the effects of informal sanctions may depend on the situation and how the organization works.

Hypothesis H5 is supported by robust empirical evidence. This finding advances our understanding of how emotions intricately shape compliance behavior. The study reveals that shame plays a constructive role in influencing employees' intentions to adhere to their organization's ISP. It implies that when employees perceive noncompliance with information security policies as a shameful act, they become more motivated to distance themselves from such behavior. This alignment with deterrence theory, which frequently incorporates shame as a self-imposed sanction, resonates with similar findings in criminology literature (e.g., Grasmick and Bursik, 1990; Nagin and Paternoster, 1993; Tibbetts, 1997). The concept of shame has been a subject of theoretical and empirical exploration in the fields of criminology and psychology. While some scholars in criminology have integrated shame within the deterrence theory framework, viewing it as a form of self-imposed sanction, others have questioned its alignment with this theoretical framework, which traditionally revolves around calculated pain avoidance. Despite these debates, research on shame as a self-conscious.

Acceptance of Hypothesis H6 deepens our understanding of the intricate relationships between "consistency culture," "moral beliefs," and "compliance intention." These findings shed light on how organizational culture plays a pivotal role in influencing employees' commitment to adhering to ISP. Figure 4 visually represents these insights, featuring three distinct lines illustrating the correlation between moral beliefs (x-axis) and ISP compliance intention (y-axis). In this graphical representation, the central line signifies the correlation within an organization characterized by an average consistency culture. Meanwhile, the other two lines represent the connection between the moderator variable, consistency culture, and higher and lower levels. The crucial observation is that all three lines exhibit a positive incline, indicating a positive correlation between higher moral beliefs and greater compliance intention among employees. However, the real significance emerges in the moderation effect. At elevated levels of the moderator, namely consistency culture, the impact of moral beliefs on compliance intention is significantly amplified. This study underscores the significant influence of organizational culture on employees' behavioral intentions, particularly by highlighting the reinforcing role of consistency culture in enhancing the positive relationship between moral beliefs and compliance intention. It's important to note that this research represents an initial empirical exploration of the moderating effect of consistency culture on the association between moral beliefs and employees' compliance intentions, thus contributing to the current body of knowledge in this field.

Hypothesis H7 posits that the presence of an effectiveness culture amplifies the positive connection between perceived benefits and the intention to comply. This hypothesis finds support through statistically significant results. To further elucidate this relationship, Figure 5 visually represents the reciprocal interplay between perceived benefits and the effectiveness culture concerning compliance intention. The

figure delineates three distinct lines that represent varying levels of effectiveness culture. The central line portrays the association between perceived benefits and compliance intention in situations where the effectiveness culture is at a moderate level. Notably, this line exhibits a positive upward trend, indicating that as perceived benefits increase; there is a stronger inclination to comply, even within an organization characterized by an average level of effectiveness culture. However, the significance of Hypothesis H7 becomes more pronounced when examining the lines corresponding to heightened and reduced levels of effectiveness culture. At elevated levels of effectiveness culture, there is a discernible enhancement in the impact of perceived benefits on compliance intention. In contrast, diminished levels of effectiveness culture result in a comparatively weaker association between perceived benefits and compliance intention. This underscores the pivotal role of an effectiveness culture in accentuating the influence of perceived benefits on employees' intentions to comply with ISP. These findings contribute valuable insights to the understanding of how organizational culture can shape employees' compliance intentions and further extend our knowledge in this domain.

Hypothesis H8 garners substantial empirical support as presented above, confirming that consistency culture plays a pivotal role in magnifying the positive impact of formal sanctions on compliance intention. Figure 6 serves as a visual representation of this dynamic, illustrating the relationship between formal sanctions (x-axis) and compliance intention (y-axis) through three distinct lines. The central line corresponds to organizations with an average level of consistency culture, flanked by two lines depicting scenarios with higher and lower levels of this cultural attribute. Figure 6 unmistakably reveals that all three lines exhibit a positive slope, signifying a favorable correlation between formal sanctions and compliance intention. In essence, the presence of formal sanctions tends to elevate employees' intention to comply with information security policies. However, the strength of this connection varies with the prevailing level of consistency culture within the organization. In settings characterized by a high consistency culture (as indicated by the upper line), the impact of formal sanctions on compliance intention is notably more pronounced. In these structured and rule-oriented environments, formal sanctions carry a heightened sense of legitimacy and efficacy. Consequently, employees are more inclined to recognize the consequences of non-compliance, resulting in a stronger intention to comply. Conversely, in organizations with lower levels of consistency culture (as depicted by the lower line), the influence of formal sanctions on compliance intention is somewhat diminished. In these less structured contexts, formal sanctions may exert a comparatively weaker influence on employees' compliance intentions. The alignment between consistency culture and formal sanctions is evident in their shared emphasis on structure, rules, and regulations. Consistency-focused organizations thrive on structured procedures and established norms, making them a natural fit for formal sanctions, which explicitly deter specific organizational misconduct. In such a culture, formal sanctions make the consequences of information security violations clear and predictable, rendering them more legitimate and effective in promoting compliance.

Hypothesis H11 is strongly supported, affirming that cooperativeness culture plays a significant role in amplifying the positive relationship between shame and compliance intention. Figure 7 offers a visual representation of these dynamic, utilizing three distinct lines to depict the association between shame (x-axis) and compliance intention (y-axis). The central line represents an organization with an average level of cooperativeness culture, while the other two lines illustrate this relationship in scenarios with higher or lower levels of cooperativeness culture.

From the graphical representation in Figure 7, it is evident that all three lines exhibit a positive slope, indicating that greater levels of shame are linked to 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. However, the moderating effect of cooperativeness culture becomes apparent, revealing that in organizations with a high level of cooperativeness culture, the influence of shame on compliance intention is significantly stronger. Conversely, in organizations with a less pronounced cooperativeness culture, the effect of shame on compliance intention is relatively weaker. This distinction underscores the substantial role played by organizational culture in either enhancing or diminishing the impact of shame as a driver of compliance intention. Cooperativeness culture, characterized by its emphasis on cooperation, trust, and teamwork, fosters an environment where individuals respond positively to feelings of shame or guilt related to non-compliance. This culture promotes collective responsibility, motivating individuals to uphold organizational standards and comply

with regulations. The connection between cooperativeness culture and shame aligns with deterrence literature, which recognizes shame as a potent mechanism for deterring undesirable behaviors. In conclusion, Hypothesis H11 emphasizes the essential role of cooperativeness culture in strengthening the positive influence of shame on compliance intention, highlighting the significance of cultivating a cooperative and supportive organizational culture to bolster compliance with policies and regulations.

Theoretical and practical contribution

The study presents a novel model that integrates non-fear-based theory which is RCT with organizational cultural theory CVF to explore employee compliance with information security policies. It emphasizes the importance of organizational cultural dimensions in evaluating the impact of deterrent countermeasures on ISP compliance. The research adopts an individual-level approach, addressing concerns of oversimplification and enriching the field of information system security research. It also explores the effects of factors like shame, moral beliefs, formal and informal sanctions, and perceived benefits across different organizational culture dimensions.

Information security managers (ISM) should consider the moral aspects of compliance and frame it as a moral duty alongside its technical aspects. Prioritize end-user involvement in policy development. Utilize effective communication and awareness campaigns highlighting organizational, personal, and ethical benefits. Implement monitoring and reporting systems for shaping compliance behavior. Collaborate with human resource and leadership to establish a consistency culture by embedding values in the organization's mission. Create a culture where reporting incidents related to non-compliance is encouraged and viewed as opportunities for learning and improvement rather than sources of shame or punishment. Organizations should cultivate a consistent and ethical culture, emphasizing ethical values and moral beliefs to enhance compliance intentions. In an effectiveness culture, stress efficiency and communicate the tangible benefits of compliance. In consistency-based cultures, clearly define and communicate formal sanctions to ensure employees understand the consequences of non-compliance. In cooperative cultures, leverage the emotion of shame to motivate compliance by promoting teamwork and cooperation. Lastly, many Ethiopian organizations lack dedicated information security departments and standardized policies. Collaboration with information network security agency(INSA) is vital to align with national initiatives for enhanced information systems and data protection. INSA in Ethiopia, responsible for national information security policies, appears to have adopted ISO 27002 without considering cultural influences, despite literature highlighting culture's role in technology practices. Our study's results can aid INSA decision-makers in shaping the current security policy.

Limitations and Future Research Directions

This study has several primary limitations that need to be considered. Firstly, similar to a majority of information systems (IS) research, the data for this study were collected from a single country. Consequently, there might be limitations in generalizing the findings to diverse countries and cultures. Future research should aim to replicate this study in various geographical and cultural contexts, encompassing both developed and developing countries, to determine the generalizability of the findings. Additionally, researchers should consider measuring culture at the individual level instead of relying solely on Hofstede's (2001) cultural values, as this may lead to more accurate assessments of organizational culture dimensions in countries with similar cultures.

A second limitation is the focus on measuring employees' intentions rather than their actual behavior. While there is typically a significant association between intentions and actual behavior, it is essential to acknowledge this limitation. Nonetheless, no theoretical justification has been found to suggest that ISP compliance behavior would differ significantly from anonymously reported intentions. The use of a scenario-based approach for assessing intention, consistent with prior studies on ISP compliance, such as those conducted by Wenzel (2004), Pahnila et al. (2007), Siponen and Vance (2010), and Vance, Siponen, & Straub (2020), should provide confidence in the study's methodology.Another limitation pertains to the scope of the selected sample, which was based solely on organizations with well-established ISPs. While this selection criterion was necessary for studying employees operating within a policy framework, it may introduce potential biases in the sample. To mitigate this, the study employed scenario-based methods to encourage more authentic responses. Additionally, similar procedures have been adopted in previous information security studies (e.g., Li et al., 2010; Vance and Siponen, 2012).

Fourth, the research model prioritizes simplicity and theoretical clarity, primarily

focusing on examining the moderating effects of Consistency culture on moral beliefs, Effectiveness culture on perceived benefits, and Consistency culture on formal sanctions in relation to compliance intention. However, additional research is needed to investigate the moderating effects of shame, perceived benefit on Consistency culture, informal sanctions, formal sanctions, perceived benefit, and moral belief on Cooperativeness culture, as well as shame, informal sanctions, formal sanctions, and moral belief on Effectiveness culture. Expanding the scope of research in these directions can provide a more comprehensive understanding of the complex interplay between organizational culture, individual beliefs, and compliance intention.In conclusion, this study employed a quantitative research method. Future research should consider supplementing the survey method with additional interviews or qualitative approaches to provide a more in-depth explanation and triangulation of the findings. These combined methodologies can offer a richer understanding of the intricate relationships explored in this study.

CONCLUSION

ISP compliance is a critical concern for organizations, and extensive research in the field of Information Systems (IS) has explored this issue using various theoretical frameworks. While previous studies have predominantly focused on fear-based strategies, they often overlooked essential variables, including shame, perceived benefits, informal sanctions, and moral beliefs. To address this research gap, our study tested a model based on Rational Choice Theory (RCT), an extension of deterrence theory, and empirically examined the moderating impact of organizational culture dimensions, namely consistency, effectiveness, cooperativeness, and innovativeness, on the relationship between RCT constructs and employees' compliance intentions toward their organization's ISP.

The empirical model presented in this study is strongly supported by the collected data, yielding significant empirical evidence regarding the factors that either hinder or facilitate employees' adherence to their organization's ISP. This study makes a substantial contribution to both research and theory, shedding light on previously understudied variables and offering practical implications for enhancing information security practices. While acknowledging the study's constraints, we also propose potential avenues for future research in the field of information security, aiming to further our understanding of the factors that influence employees' behavior concerning information security. In conclusion, this research advances our comprehension of ISP compliance, emphasizing the importance of examining a broader set of factors and organizational culture dimensions to develop more effective information security strategies.

REFERENCES

1. Bulgurcu, B., et al. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 523-548.
2. Carlsmith, K. M., et al. (2002). Why do we punish? Deterrence and just deserts as motives for punishment. *Journal of personality and social psychology, 83*(2), 284.
3. 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.
4. Cram, W. A., et al. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems, 26*, 605-641.
5. D'Arcy, J., et al. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security, 22*(5), 474-489.
6. D'arcy, J., et al. (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.
7. 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.
8. 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.
9. Ejigu, K., et al. (2021). *Influence of Organizational Culture on Employees Information Security Policy Compliance in Ethiopian Companies*. Paper presented at the Pacific Asia Conference on Information Systems.

10. 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.
11. Ernest Chang, S., et al. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438-458. doi:10.1108/02635570710734316
12. 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*.
13. Herath, T., et al. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*, 106-125.
14. Herath, T., et al. (2017). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125. doi:10.1057/ejis.2009.6
15. 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.
16. 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.
17. 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.
18. Johnston, A. C., et al. (2016). Dispositional and situational factors: influences on information security policy violations. *European Journal of Information Systems, 25*(3), 231-251.
19. Karjalainen, M., et al. (2013). One size does not fit all: different cultures require different information systems security interventions.
20. Karlsson, M., et al. (2022). The effect of perceived organizational culture on employees' information security compliance. *Information & Computer Security, 30*(3), 382-401.
21. Kaviani, F., et al. (2020). Understanding the deterrent impact formal and informal sanctions have on illegal smartphone use while driving. *Accident Analysis & Prevention, 145*, 105706.
22. Latan, H., et al. (2017). Partial least squares path modeling. *Partial least squares path modeling: basic concepts, methodological issues and applications*.
23. Moody, G. D., et al. (2018). Toward a unified model of information security policy compliance. *MIS quarterly, 42*(1).
24. 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.
25. 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.
26. Paternoster, R., et al. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law and Society Review*, 549-583.
27. Pogarsky, G. (2009). Deterrence and decision making: Research questions and theoretical refinements. *Handbook on crime and deviance*, 241-258.
28. Roberts, D. J. (2021). *An Analysis of Employee Information Security Policy Compliance Behavior: A Generic Qualitative Inquiry.* Capella University,
29. Siponen, M., et al. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64-71.
30. Siponen, M., et al. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502.
31. Solomon, G., et al. (2021). The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management, 34*(4), 1203-1228.
32. Sommestad, T., et al. (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.
33. 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

34. 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.
35. Streukens, S., et al. (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.
36. Tadesse, K., et al. (2021). Influence of Organizational Culture on Employees' Compliance with Information Security Policy: Ethiopian and Finland Companies.
37. Tang, M., et al. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management, 17*, 179-186.
38. Tangney, J. P., et al. (2002). Gender differences in morality.
39. Tarafdar, M., et al. (2014). The dark side of information technology. *MIT Sloan Management Review*.
40. Tilahun, A., et al. (2017). Influence of national culture on employees'intention to violate information systems security policies: a national culture and rational choice theory perspective.
41. Tyler, T. R., et al. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of management journal, 48*(6), 1143-1158.
42. Van Niekerk, J., et al. (2010). Information security culture: A management perspective. *Computers & Security, 29*(4), 476-486.
43. 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
44. Vance, A., et al. (2012). IS Security Policy Violations. *Journal of Organizational and End User Computing, 24*(1), 21-41. doi:10.4018/joeuc.2012010102
45. Vance, A., et al. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. *Information & Management, 57*(4), 103212.
46. Von Solms, B. (2006). Information security–the fourth wave. *Computers & Security, 25*(3), 165-168.
48. Vroom, C., et al. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198. doi:10.1016/j.cose.2004.01.012
49. Wenzel, M. (2004). The social side of sanctions: Personal and social norms as moderators of deterrence. *Law and human behavior, 28*, 547-567.
50. Willison, R., et al. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS quarterly*, 1-20.
51. Xu, H., et al. (2019). Earnings management in firms with data security breaches. *Journal of Information Systems, 33*(3), 267-284.
52. Zeb, A., et al. (2021). The competing value framework model of organizational culture, innovation and performance. *Business process management journal*.