SINET: Ethiop. J. Sci., 44(1):108–118, 2021 ISSN: 0379–2897 (PRINT)
© College of Natural and Computational Sciences, Addis Ababa University, 2021 eISSN: 2520–7997

DOI: https://dx.doi.org/10.4314/sinet.v44i1.10

Factors influencing information security compliance: an institutional perspective

Temtim Assefa [1, *] and Alpha Tensaye [2]

[1] School of Information Science, Addis Ababa University, Addis Ababa, Ethiopia.
E-mail: temtim.assefa@aau.edu.et
[2] Ethiopian Telecommunication Corporations

ABSTRACT: Information is the critical resource of modern organization that needs to be protected from both internal and external threats so as to sustain in this competitive business environment. In order to do so, comprehensive security policy must be formulated and implemented. Every employee of the organization must comply with the organization's security policy. Although organizations implement information security policy, it is commonly observed that employees do not comply with the organization information security policy. The purpose of this research was to identify organizational factors that shape employees behavior to comply with information system security policy in Ethio-telecom. Data were collected via using survey method. Multiple linear regression was used as data analysis method. The study result showed that management support, awareness and training, and accountability are leading organizational factors that shape employees behavior to comply with the existing information system security policy. This is a single case study; it cannot be generalized for other organizations. Other researchers can replicate this research for generalizability of the research findings across different contexts.

Keywords/phrases: Developing country, Information security, Information security compliance, Information security policy, Public organization

INTRODUCTION

Information is the critical resource of today's organization. As a result, organizations established information systems to manage their information resources. These systems are interconnected internally and globally so as to quickly process and share information to potential users. However, this interconnection exposes organizations to different information security threats (Bulgurcu *et al.*, 2010). Information security threats occur during storage, processing and communication of information (Kim & Solomon, 2018). Organizations must implement comprehensive security prevention mechanisms that maintain the safety of information at all levels of information management. There is now a good awareness about the benefit of information system security (Siponen, 2010).

Most of the information system security threats comes from employees unintentional and intentional actions (Alotaibi & Furnell, 2016). Empirical evidence shows that more than 70 percent of security threats come from insiders rather than from external agents (Jouini, Ben, Rabai, & Ben, 2014).This problem is usually associated with lack of knowledge about information security policies implemented in the organizations (Whitman & Mattord, 2012). As a result, employees are not aware about the consequences and damages of violating information security policy and procedures.

Information security protection mechanisms can be viewed as technical and behavioral solutions (Pavlov & Karakaneva, 2011). Technical solution includes use of passwords, assigning access rights, installation of network intrusion detection and prevention system (IDPS) and firewalls as an example. On the other hand, behavioral protection mechanisms are development of information security policy, awareness and training and risk monitoring. Punishment of employees who violate information security prevention mechanisms and rewarding those who comply with prevention mechanisms were also used as behavioral solutions (Alotaibi & Furnell, 2016).

Organizations develop and implement information system security policy (ISSP) as a comprehensive solution to information system security (Alotaibi & Furnell, 2016). Information security policy is a formal document that describes acceptable and unacceptable behaviour of users

[*] Author to whom correspondence should be addressed.

while accessing organizational information and IT resources (Alotaibi, Furnell, & Clarke, 2017). It is a set of guidelines, procedures and standards that must be followed by employees to ensure security of information resources and other technological devices (Bulgurcu *et al*., 2010). It is an organization official document approved by top management and then distributed and communicated to all employees (Alotaibi *et al*., 2017). There is no one standard policy applicable to all organization rather it is developed by organizations to address their specific information security requirements (Antoniou, 2015).

ISSP has different contents depending on the need of the organization. Main contents included (i) purpose of policies, (ii) scope which describe the people affected by the policy, the infrastructure and information systems to which the policy applies, (iii) establishment of role and responsibilities, (iv) sanctions and violations, which includes how policy violation should be reported, and what sanctions should be taken in case of policy violation and (v) history of revisions, which defines the person responsible for making updates and revisions, and how often they need to be done (Kamariza, 2017). Although ISSP is written as clear as possible, there is a challenge to comply to rules and regulations mentioned in the policy document by employees (Alotaibi *et al*., 2017; Bulgurcu *et al*., 2010). This issue is still a hot research agenda to identify factors that shape employees behaviour to act in accordance with ISSP. However, there is also inconsistent findings in the current literature (AlKalbani, Deng, Kam & Zhang, 2017; Bulgurcu *et al*., 2010). This creates a knowledge gap for practitioners to make decisions on the selection and implementation of appropriate actions to bring information security compliance among their employees. Most of the studies were organization based or country specific which cannot be generalized to other context without undertaking similar empirical research (Siponen, 2010). Therefore, this study was undertaken to investigate factors that shape employees' behavior to act in line with the organization ISSP at Ethiopian Telecommunication Corporation (Ethiotelecom).

Ethiotelecom is the only and largest telecom service provider in the country with 8,441 for employees, 25.57 Billion ETB annual revenue and more than 50.7 million customers as of June 2020 (Ethiotelecom, 2021). Mobile voice subscribers reached 48.9 million, Data and Internet users reached 23.5 million, Fixed Telephone subscribers are 981, 000 and Fixed Broadband subscribers reached 309.400.

Information security issue is now every country concern. Ethiopia has established Information Network Security Agency (INSA) in 2006 with council of ministers regulation No. 130/2006 (Getaneh, 2018). The main objective of the Agency was to ensure the safe use of the country's information and information communication network technologies and telecommunication. In addition, INSA supporting government organizations by developing and distributing cyber security enforcement standard called Critical Mass Cyber Security Requirement Standard (CMCSRS) which was issued as Version 1.0 in September 2017 (Getaneh, 2018). The standard was distributed for implementation by public organizations including Ethiotelecom to build their cyber security capabilities and implement cyber security prevention mechanisms.

According to discussion with security expert at Ethiotelecom, the Corporation has Information Security Department since the release of CMCSRS by INSA. The Department is now upgraded to Information Security Division with four departments since 2020. It has more than 200 employees in the Division. However, there is no staff qualified with information security field. All are IT gradates but upgrade their knowledge and skills of information security management with short term training facilitated by the Corporation. Even the short term certification trainings were not provided to all staff of the Division (Getaneh, 2018). The Corporation has approved information security policy document based on the national cyber security standard (CMCSRS) (Expert Interview in Information System Security Division, April 11, 2021).

Therefore, this research has addressed the following research question.

- What organizational factors shape employees behaviour to comply with the organization's ISSP at Ethio-telecom?

The paper is organized by the following structure. Section two discuses methods and materials used to undertake the research. It then presents results of empirical data. Finally, it winds up by discussing main research findings and future research directions.

MATERIALS AND METHODS

A research methodology is a systematic approach to address a research problem from the theoretical underpinning of the research to the collection, analysis and interpretation of the data (Kothari 2004). This research used a survey research method. It is a quantitative research approach which involves counting and measuring variables using numbers to explain certain answers. It also allows us to get data from large sample population.

Explanatory studies are valuable when studies are meant to establish causal relationships between independent and dependent variables (Saunders *et al*., 2007). Yin (2009) adds that explanatory study is used as a means to answer 'how' and 'why' questions and get answers, especially for the case study research method. This research was undertaken to examine employees' information security compliance in a single organization.

Research Model

Previous research on cyber security compliance posits that cyber security compliance can be influenced and impacted by technical measures/ controls; accountability; monitoring and control and end-user awareness (Alqahtani & Braun, 2021). By reviewing previous literature, this researcher identified management commitment, awareness and training, accountability, and audit and monitoring as organizational factors that influence employees' compliance to ISSP.

Management commitment

Management commitment refers to the decisions, investments and actions taken for enforcing information security policies across the organization (Knapp *et al*. 2006). It centers on the efforts of senior management to promote an information security culture in organizations for information security compliance (Kajava *et al.* 2007). Management commitment directly affects employee's behaviors to comply with information security policies and standards (Dhillon & Backhouse 2001). Having visible management participation and ongoing communication on information security stimulate employees to follow acceptable behaviors as articulated in ISSP document (Kolkowska & Dhillon, 2012). The creation, training and enforcement of organization's information system security policies would not be taken seriously without top management support and involvement (Chopra & Chaudhary, 2020). In fact, lack of management support to encourage adherence to information security policies has been singled out as a common reason for employees' failure to comply with information security policy standards and procedures (Alotaibi *et al*., 2017; Kolkowska & Dhillon, 2012). Therefore, it is hypothesized that

H1: Management commitment has positive influence on employee's compliance to ISSP

Accountability

Accountability refers to the level of understanding of employees to take responsible actions in accordance with the organization's information system security policy (Alqahtani & Braun, 2021). It emphasizes on individuals' roles and responsibilities towards enforcing information security in organizations (HerathRaghav & Rao, 2009). Accountability increases if employees know (a) comprehensiveness of information security policies for guiding appropriate information security compliance behaviors (Chan *et al.* 2005a), (b) clarity and understandability of roles and responsibilities (Bulgurcu *et al.* 2010), (c) appropriateness of sanctions for violating information security policies (HerathRaghav & Rao, 2009), and (d) enforcement of information security policies and procedures across the organization (Alqahtani & Braun, 2021).

Well-defined roles and responsibilities of individual employees are useful in guiding employees to be more proactive in undertaking higher information security precautions (Al-Kalbani *et al.* 2015). Clarity of sanctions for information security breaches in organizations encourages individuals to comply with information security policies and standards (Adams and Sasse, 1999; Bulgurcu *et al.* 2010). Previous studies have consistently indicated that if employees are held responsible for some action, they will behave in a socially unacceptable manner (Alqahtani & Braun, 2021). Accountability increases employees' positive attitude to avoid unacceptable behaviors and comply with ISSP (HerathRaghav & Rao, 2009). Therefore

H2: Accountability has a positive influence on employees' compliance to ISSP

Awareness and training

Information security awareness and training is defined as a form of knowledge sharing to increase employee's knowledge and understanding about the organization's ISSP (Bulgurcu *et al.*, 2010).This is because such programs can raise users' knowledge and understanding of security policies and mechanisms in organizations (Puhakainen & Siponen 2010). The presence of information security awareness programs increases employee's beliefs about the benefit of compliance and the cost of noncompliance for information security (Bulgurcu *et al.*, 2010).

The availability of awareness and training programs in the organization can raise the knowledge and skills of employees with respect to the information system security policies and prevention mechanisms (Bulgurcu *et al.*, 2010; Kim & Solomon, 2018). The usefulness of the training is assessed by examining how well the awareness and training programs are structured and presented (Barling *et al.* 2002). The training should include topics regarding your organization's regulatory compliance and legal requirements (Kim & Solomon, 2018). It can also reduce the misuse of information security policies and procedures and increase users' avoidance of information security risks and threats (Tsohou *et al.*, 2008). Therefore, it can be hypothesized that

H3: awareness and training program has a positive influence on employees' compliance to ISSP

- ***Audit and monitoring***

Audit and monitoring is a managerial process to oversee and control employees if they are acting according to the organizations information security policy and procedures. Developing effective audit and monitoring processes is critical for information security compliance (Kolkowska & Dhillon 2012; Neubauer *et al.* 2006). Security audit is used to make sure your systems and security controls work as expected (Kim & Solomon, 2018). The influence of audit and monitoring processes for information security compliance in organizations can be assessed by employees' perceptions on various features such as the appropriateness of audit and monitoring activities in terms of time and place suitability (Knapp *et al.* 2006). Regular audit and monitoring processes help to check security controls are current and effective (Kim & Solomon, 2018). It also raises the speed of operational execution of information security mechanisms and improves the overall effectiveness of information security mechanisms (Ransbotham & Mitra 2009). Kolkowska and Dhillon (2012) assert that audit and monitoring processes could improve information security compliance in organizations. Employees believe that effective monitoring of misuse would increase the likelihood of compliance (Alotaibi & Furnell, 2016). It can be hypothesized that

H4: audit and monitoring will have a positive influence on employees compliance to ISSP

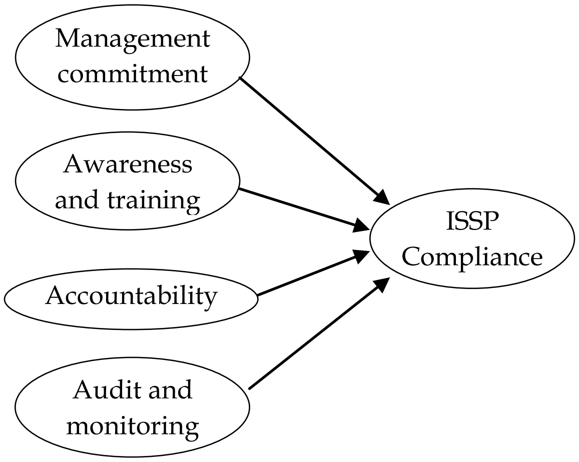

Figure. 1 Research Model of ISSP compliance

Source: adapted from (Alqahtani & Braun, 2021)

- ***Information security compliance***

Information system security compliance is defined as employees' adherence to organizational information security policy and procedures while using the information system (AlKalbani *et al.*, 2017). Employees compliance to ISSP indicates that employees act within the framework of the policy while they access and use information systems and communicate with other colleagues within and outside the organization (Bulgurcu *et al.*, 2010). Employee compliance to information security indicates effectiveness of the implemented information system security policy and procedures while noncompliance indicates rejection of implemented ISSP. ISSP should not be restrictive and create barrier to accomplish employees' daily tasks (Antoniou, 2015).

Instrument development

Data collection instruments are used to measure the research variables. The instruments were extracted from existing information system security literature (see Table 1). After developing the instruments, pilot testing was conducted with 10 respondents who are working in Ethio-telecom. These respondents were excluded in the main survey to avoid any bias. During pilot testing, respondents were told to check all aspect of the questionnaire such as content validity, clarity of questionnaire, questions order and redundancy of questions.

Table 1. Data collection instruments.

Variable	Operational definition	Indicators
Management commitment	Management commitment refers to the decisions, investments and actions taken for enforcing information security policies across the organization (Knapp *et al*. 2006	1. I know that senior managements promote an information security culture (Kajava *et al*. 2007). 2. I know that senior managers encourage employee to comply with information security policies and standards (Dhillon & Backhouse 2001) 3. I know that senior managers communicate information system security policy to employees (Kolkowska & Dhillon, 2012) 4. I know that senior managers actively participate in creation, training and enforcement of organization's information system security policy (AlKalbani *et al*., 2017) (Chopra & Chaudhary, 2020)
Accountability	Accountability refers to the level of understanding of employees to take responsible actions in accordance with the organization's information system security policy (Alqahtani & Braun, 2021)	1. I know that information system security policy clearly describes individuals' roles and responsibilities (Bulgurcu *et al*. 2010) 2. I know that information system security policy states sanctions for non compliance behaviour (HerathRaghav & Rao, 2009) 3. I know that accountability increases positive attitude for information system security compliance (HerathRaghav & Rao, 2009)
Awareness and training	Information security awareness and training is defined as a form of knowledge sharing to increase employee's knowledge and understanding about the organization's ISSP (Bulgurcu *et al*., 2010)	1. I know that trainings provided in my organization raises my knowledge and understanding of ISSP (Puhakainen & Siponen 2010). 2. I know that awareness programs increase my beliefs about the benefit of ISSP compliance (Bulgurcu *et al*., 2010). 3. I know that awareness and training programs reduce the misuse of information security policies and procedures (Tsohou *et al*., 2008). 4. I know that training contents are relevant to increase my understanding and knowledge about information security (Stephanou & Dagada, 2014)
Audit and monitoring	Audit and monitoring is a managerial process to oversee and control employees if they are acting according to the organizations information security policy and procedures	1. I know that audit and monitoring processes are effective to increase information security compliance (Kolkowska & Dhillon 2012) 2. I know that existing monitoring processes increase my understanding to comply with ISSP (Alotaibi & Furnell, 2016) 3. I know that presence of audit and monitoring processes influences my behaviour to comply with ISSP (Alqahtani & Braun, 2021)
Information system security compliance	Information system security compliance is defined as employees' adherence to organizational information security policy and procedures while using the information system (AlKalbani *et al*., 2017).	1. I follow ISSP rules and procedures while communicating with other colleagues within and outside the organization (Bulgurcu *et al*., 2010). 2. I protect information and technology resources according to the requirements of the ISSP of my organization organization (Bulgurcu *et al*., 2010). 3. I understand that ISSP is not restrictive to access information resources in my organization (Antoniou, 2015).

Information obtained during pilot testing was incorporated to produce the final version of the questionnaire. The questionnaire has two main sections. Section one asked demographic information about the respondents. This includes gender, educational level, work experience and position held in the Company. Section two includes instruments developed to measure the research variables.

Population and Sampling Methods

The research was conducted on Ethio-telecom which is one of the largest organizations in Ethiopia having branch offices all over the country. From all ethio-telecom branch offices, four branch offices at Addis Ababa were selected by using random sample method. Then we collected the list of employees who are working in the selected branch offices. The list of employees was organized by department and representative samples were selected from each department. Then we applied systematic sampling methods to select questionnaire respondents. We used Solvin's formula to determine the sample size. The total number of employees in four branches was 500. Of which 223 samples were selected using 5% margin error and 95% level of confidence (Kothari, 2004).

Method of Data Analysis

Both descriptive and inferential statistical methods were used to undertake data analysis. Inferential statistical methods were used to test hypothesis. Linear regression was used to measure the effect of independent variables on employees' compliance to ISSP. Before we apply linear regression, we transform each variable's multiple values into single continuous value using summation method. Statistical Package for the Social Sciences (SPSS) version 25 was used as data analysis tool. SPSS generated different reports of linear regression, i.e Model summary table to assess the overall effect of the independent variable on the dependent variable and ANOVA table to check statistical significance of the model. Linear regression also used to rank independent variables by their influence on the dependent variables so that organizations will focus to take interventions on variables which have more influence on the dependent variable.

RESULTS AND DISCUSSION

Results

A total of 223 questionnaires were distributed to selected sample respondents. Of which 177 questionnaires were properly filled and returned. The other 40 respondents did not return the questionnaire and 6 respondents' questionnaires were not properly filled and discarded from being included in the data processing. The response rate was 79%. This was a good response rate and did not violate our sampling assumption.

To validate the measurement model Cronbach's alpha was used. When we add all items, the alpha value was 0.799. After removing one question item which has a negative correlation value in the inter-item correlation result, its value increased to 0.819 (see Table 2). The minimum acceptable alpha value for reliable instrument is 0.7 (Pallant, 2005).

Table 2. Reliability Statistics.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.818	.819	16

Demographic characteristics

Respondents' demographic information includes employee's age, gender, department, educational status and experience with computers. These data were included to show data was collected from different demographic characteristics so as to avoid any bias that may occur when respondents were selected from only one group.

When we see the respondent by their age 56.5% of the respondents were found in the age range of 26-35 years and then followed by employees in the age range of 36-45 and 20-25 years with 19.2% and 13.0%, respectively.

When we look at respondents by gender, we found almost similar distribution. About 49.7% are male respondents while the other 48.6% are females. This data did not have any gender bias errors. Examining the educational background of the respondents, majority of the respondents are bachelor degree holders with percentage of 84.7% while 13.0% of the respondents have masters degree. This implies that respondents are well educated to understand information security policy documents and comply with the organizational security expectation.

When we see the respondents by their experience with computers, 46.9% of the respondents reported that they have satisfactory experience with computers while 33.9% of the respondents have sufficient experience and 18.6% of the respondents have moderate experience with computers. This indicates that most of the employees manage their information using computers and they are likely to be exposed to information system security risks.

Hypothesis testing

Before we applied linear regression to test the hypothesis, we checked the data if it meets the assumption of linear regression. One of the assumption is that the independent and dependent variables should show some relationship which is preferably above 0.3 correlation value (Pallant, 2005). In this regard, the three independent variables have more than 0.3 correlation value. However, auditing and monitoring has only 0.19.

Tabachnick and Fidell (2001, p. 84) suggest that you 'think carefully before including two variables with a bivariate correlation of, say, 0.7 or more in the same analysis'. Higher correlation may indicate presence of multicollinearity problem. The correlation results of the variables show that all have below 0.56, which is less than 0.7. As a result, all variables were retained for the analysis.

Multiple linear regression requires the dependent variable to have a normal distribution. We used normality plot diagram to check its normality. Normal Probability Plot diagram shows that all points lie in a reasonably straight diagonal line from bottom left to top right. The research data meets the normality assumption of multiple linear regression requirements (see Figure 2).

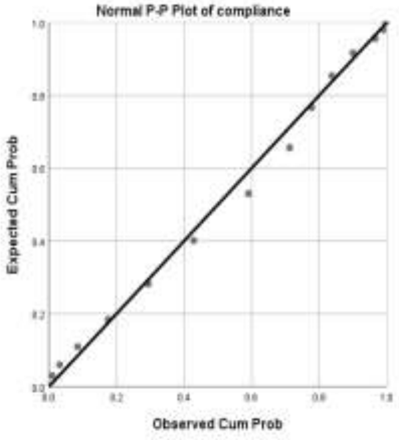

Figure 2. Normality Plot diagram for security compliance variable

Multicollinearity is an issue to be addressed well in linear regression. There are two parameters we check for presence or absence of multicollinearity: Tolerance and variance inflation factor (VIF) (Tabachnick & Fidell, 2013). Tolerance is an indicator of how much of the variability of the specified independent variable is not explained by the other independent variables in the model and is calculated using the formula $1–R^2$ for each variable. If this value is very small (less than .10), it indicates that the multiple correlation with other variables is high, suggesting the possibility of multicollinearity (Pallant, 2005). The other value given is the VIF, which is just the inverse of the Tolerance value (1 divided by Tolerance). VIF values above 10 would be a concern here, indicating multicollinearity. Our data results indicate that there is no multicollinearity problem. All variables Tolerance is above 0.7 and their VIF's values are below 2.

The model summary table shows the overall impact of the independent variables on the dependent variables (i.e. employee compliance to the information system security policy). All the four variables can explain 47.2 percent of changes on the dependent variables (see Table 3).

Table 3. Model summary.

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.687[a]	.472	.454	2.22757

a. *Predictors: (Constant), auditing and monitoring (AM17), accountability, awareness and training (ATraining), management commitment (Mcommitment)*
b. *Dependent Variable: compliance*

To assess the statistical significance of the result, we used the ANOVA table. The model in this study has statistical significance value of $p < .0005$(Sig = .000). The model represents the relationship among variables in the real world.

Table 4. Statistical significance the of Model.

ANOVA[a]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	536.297	4	134.074	27.020	.000[b]
	Residual	600.409	121	4.962		
	Total	1136.706	125			

a. Dependent Variable: compliance

b. Predictors: (Constant), AM17, accountability, ATraining, Mcommitment

In order to check the contribution of each independent variable to the prediction of the dependent variable, we use the coefficient table which reports beta value of standardized coefficients. The standardized column shows the converted value of each independent variables into the same scale so that we can compare them (Pallant, 2005).

Table 5. Contribution of each of the independent variable to dependent variables.

Coefficients[a]

Model	Unstandardized Coefficients		Standardized Coefficients	T	Sig.	Collinearity Statistics	
	B	Std. Error	Beta			Tolerance	VIF
(Constant)	-1.813	1.363		-1.331	.186		
ATraining	.332	.081	.309	4.077	.000	.761	1.314
Mcommitment	.319	.075	.329	4.241	.000	.723	1.382
accountability	.266	.069	.264	3.844	.000	.923	1.083
AM17	.406	.178	.153	2.277	.025	.967	1.034

a. Dependent Variable: compliance

Management commitment is the first to influence employee's compliance to ISSP with 32.9 percent of contribution. Its statistical significance is less than 0.001. Therefore, Hypothesis 1 is accepted (see Figure 3). Managers can shape their employees behaviour by being role models to accept and act according to the information security policy and procedures. They also provide the necessary facilities such as arranging training programs, organizing awareness workshops and seminars and allocating the necessary budgets and resources for the successful implementation of the ISSP in the organization. Maintaining the safety of organizational information and technological resources is the prime task of managers in order to increase the confidence of the stakeholders while they interact with the organization. This has big impact to build the image of the organization in the present digital society as most of the information is managed through electronic forms.

The second important influencing factor is awareness and training program with 30.9 percent. Its statistical significance is less than 0.001. Hypothesis 3 is also accepted (see Figure 3). Communication of security policy and procedures is critical for information security compliance. Through awareness and training program, employees get adequate information about what is the right and wrong actions while they interact with the information system. This program should be also continuous activity. As security threats are dynamic, continuous communication about information system security prevention mechanisms help to increases employees' knowledge and skills about information system security and consequently their compliance to ISSP.

Accountability is the third influencing factor with 26.4 percent (see Figure 3). Its statistical significance is less than 0.001. Hypothesis 2 is also accepted. Information security is everyone's responsibility. It has influence to increase employees' intrinsic motivation to comply with information security. If employees are accountable for their action, they consider any organizational problems as their own personal problem. They will not have the courage to take actions that endanger the organization information resources. Organization should focus to clearly communicate roles and responsibilities while they use organization information use and technological devices so as to increase their accountability to information system security.

Auditing and monitoring has also influence on ISSP compliance but it is the least one as compared to other independent variables. Its statistical significance is less than 0.05. Hypothesis 4 is also accepted. Employees may not be happy to be monitored while they are interacting with the information system. Rather they may be interested to be supported by other interventions such as security training, management support and acquisition of security prevention tools. This implies that too much auditing and monitoring will not have much influence to maintain employee's compliance to ISSP.

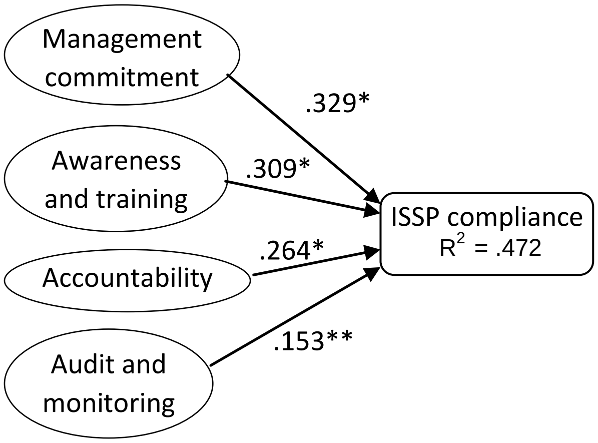

Figure 3. Research Model with empirical values

*Note:- * P<0.05, ** P<0.001*

However, the overall model explains only 47 percent of the change on the dependent variable. The other 53 percent of changes are explained by other variables which are not considered in this research model. This calls for further research to increase the predictive power of the research model.

Discussion

The purpose of this research was to examine the influence of organizational factors on employees' compliance to ISSP. Management commitment accounts for 32.9 percent of variation on ISSP. Prior research also found a positive influence of management commitment on information system security compliance (AlKalbani *et al*., 2017; Bulgurcu *et al*., 2010). This research revealed that management commitment is the top predictor to ISSP compliance than other organizational factors.

Awareness and training program is the second important factor to influence employees' behaviour to information system security compliance. It has 30.9 percent of contribution to influence information system security compliance. This finding confirms the previous research findings on awareness and training program (Alotaibi & Furnell, 2016; Bulgurcu *et al.*, 2010). Awareness and training program bring behavioral change among employees by increasing their knowledge and skills on information system security (Siponen, 2010). Introduction of new ISSP must be supported through awareness and training to enable employees understand what is expected from them to act according to the organization expectation while they use the information system and share information with other colleagues. In other words, when employees acquire the necessary knowledge and skills about information security, they will likely to comply to the organization information system security policy and procedures (Alotaibi & Furnell, 2016). Organizations must be aware that when new employees are hired, they have to provide information system security training to develop their understanding about ISSP rules and procedures. It also clarifies their roles and responsibilities expected by the organization.

Accountability is the third important factor to influence information system security compliance with 26.4 percent of unique contribution to variances on ISSP compliance. Accountability creates intrinsic motivation among employees to behave according to the organization information system security policy and procedures (Tsohou *et al.* 2008). Accountability increases employees' positive attitude to achieve information security compliance (Herath and Rao, 2009).

This research found that audit and monitoring has an influence on ISSP compliance. Security audit is used to make sure your systems and security controls work as expected (Kim & Solomon, 2018). This research finding is also in line with the previous research finding (Kolkowska & Dhillon, 2012). Audit and monitoring processes improve information system security compliance in organizations by providing real time information about unacceptable behaviour of employees while using organizational information resources and technological devices and to take timely actions. Employees believe that effective monitoring of misuse would increase the likelihood of information system security compliance (Alotaibi & Furnell, 2016).

CONCLUSION

The purpose of this research was to identify organizational factors that influence employees' behaviour to comply with ISSP. This study identified management commitment, awareness and training, accountability and audit and monitoring as dimensions of of organizational factors. The research revealed that all factors identified as organizational factors positively influence employees behaviour to comply with ISSP. Specifically, this study demonstrates that management commitment is the first factor to influence employees' behavior to comply with ISSP and then followed by awareness and training program and accountability. Audit and monitoring has low influence as compared to other factors

Current research on information security compliance is fragmented. There is no grand theory that can be used as lens to study information security compliance. This research has a theoretical contribution to increase our understanding about factors that influence employees' behavior on information system security compliance from organizational perspective. This research also contribution by developing and validating data collection instruments to measure organizational factors.

This research has limitation. It is undertaken on single organization in one country. Therefore, it cannot be generalizable to other organizations and countries. Other researchers can replicate the study to other public organizations to make the research findings generalizable across different contexts. The research also explains only 47 percent of the variation on ISSP compliance. Other researchers can add technical and individual factors in the research model to increase the research model's predictive power.

REFERENCES

1. AlKalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Compliance in Organizations : An Institutional Perspective What Is So Different About Was ist so anders am Neuroenhancement ? *Data and Information Management*, *1*(2). https://doi.org/https://doi.org/10.1515/dim-2017-0006

2. Alotaibi, M., Furnell, S., & Clarke, N. (2017). Information security policies: A review of challenges and influencing factors. In *2016 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016* (pp. 352–358). https://doi.org/10.1109/ICITST.2016.7856729

3. Alotaibi, T., & Furnell, S. (2016). Assessing Staff Acceptance and Compliance with Information Security. *International Journal of Computing Academic Research* **5:** 195–201.

4. Alqahtani, M., & Braun, R. (2021). Examining the Impact of Technical Controls , Accountability and Monitoring towards Cyber Security Compliance in E-government Organizations. https://doi.org/DOI: 10.21203/rs.3.rs-196216/v1

5. Antoniou, G. (2015). *Designing an effective information security policy for exceptional situations in an organization: An experimental study. Dissertations.* Nova Southeastern University. Retrieved from https://login. pallas2.tcl.sc.edu/login?url= https://search.proquest.com/docview/1789310139?accountid=13965%0Ahttp://resolver.ebscohost.com/openurl?ctx_ver=Z39.88-2004& ctx_enc=info:ofi/enc: UTF-8&rfr_id=info:sid/ ProQuest+Dissertations +%26+Theses+Global&rft_v

6. Appari, A., & Anthony, D. (2009). HIPAA Compliance : An Institutional Theory Perspective HIPAA Compliance : An HIPAA Compliance : An Institutional Theory Perspective, (May 2014).

7. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly: Management Information Systems*, *Spec.issue* ***34***:523–548. https://doi.org/10.2307/ 25750690

8. Chopra, A., & Chaudhary, M. (2020). *Implementing an Information Security Management System. Implementing an Information Security Management System.* https://doi.org/10.1007/978-1-4842-5413-4

9. Ethiotelecom. (2021). Ethio telecom 2013 EFY (2020/21) First Half Business Performance Summary Report. Retrieved April 14, 2021, from https://www.ethiotelecom.et/ethio-telecom-2013-efy-2020-21-first-half-business-performance-summary-report/

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

11. Goutam, R. K. (2015). Importance of Cyber Security ***111***: 14–17.

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

13. Jouini, M., Ben, L., Rabai, A., & Ben, A. (2014). Classification of Security Threats in Information Systems. *Procedia - Procedia Computer Science*, **32:** 489–496. https://doi.org/10.1016/j.procs.2014.05.452

14. Kamariza, Y. (2017). *Implementation of information security policies in public organizations : success factor*. Jonkoping University.

15. Kim, D., & Solomon, M. G. (2018). *Fundamentals of Information Systems Security* (3rd ed.). Jones & Bartlett Learning, LLC, an Ascend Learning Company.

16. Kolkowska, E., & Dhillon, G. (2012). Organizational power and information security rule compliance. *Computers & Security*, **(33):** 3–11.

17. Kothari, C. R. (2004). *Research Methdology: Methods and Techniques*. New Delhi: New Age International Ltd.

18. Pallant, J. (2005). *SPSS survival manual: A step by step guide to data analysis using SPSS for Windows (Version 12)*. Sydney: Bookhouse.

19. Pavlov, G., & Karakaneva, J. (2011). Infromation Secruity Management System in Organization. *Trakia Journal of Sciences* **9:** 20–25.

20. Siponen, M. (2010). Improving Employees ' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, **34** 757–778.

21. Stephanou, A. & Dagada, R. (2014). The impact of information security awareness training on information security behaviour: The case for further research. *Information Security* **22***:* 309–330.

Tabachnick, B. & Fidell, L. (2013). *Using Multivariate Statistics* (6th ed.). Boston: Pearson Education, Inc.

23. Whitman, E., Mattord, J. (2012). *Principles of Information Security Fourth Edition* (4th ed.). Boston: Course Technology.