ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES SCHOOL OF INFORMATION SCIENCE

[FACTORS AFFECTING INFORMATION SYSTEMS SECURITY INVESTMENT IN SELECTED PUBLIC ORGANIATIONS IN ETHIOPIA]

By Eden Zewdie

ID: GSR/9048/14

A Thesis submitted to Addis Ababa University, College of Natural and Computational Sciences School of Information Science in partial fulfillment of the requirements of the degree of Master of Science in Information Science and Systems (Information Systems Specialization)

Advisor: Lemma Lessa (PhD.)

June 2023

Addis Ababa, Ethiopia

FACTORS AFFECTING INFORMATION SYSTEMS SECURITY INVESTMENT IN SELECTED PUBLIC ORGANIATIONS IN ETHIOPIA

By Eden Zewdie

ID: GSR/9048/14

Approved by Board of Examiner

Lemma Lessa (PHD.)		
Research Advisor	Signature	Date
Internal Examiner	Signature	Date
External Examiner	Signature	Date

Declaration

This thesis has not previously been accepted for any degree and is not being concurrently submitted in candidature for any degree in any university. I declare that this thesis entitled "*Factors Affecting information systems security investment in selected public organizations in Ethiopia*" is a result of my own investigation, except where otherwise stated. I have undertaken the study independently with the guidance and support of my research advisor. Other sources are acknowledged by citations giving explicit references. A list of references is appended.

Researcher's Name	Signature	Date
Eden Zewdie		

Certificate

This is to certify that the thesis entities "*Factors Affecting information systems security investment in selected public organizations in Ethiopia*.", submitted to Addis Ababa University, School of Information Science for the award of degree in Master of Science in Information Science and Systems (Information Systems Specialization) and is a record of bona fide research work carried out by Ms. Eden Zewdie, under my guidance and supervision. Therefore, I hereby declare that no part of this thesis has been submitted to any other university or institution for the award of any degree or diploma.

Advisor Name	Signature	Date
_____	_____	_____

Acknowledgment

Prior to anything else, I would like to express my profound gratitude to Holy Virgin Mary and Almighty God for their supremacy and being my refuge and for his promise in Isaiah 40:29-31. This epic path could not have been possible without my family, friends and my advisor helping hands. Thank you to my family for encouraging me to purse my aspirations. I'm forever grateful to my mom who supported me in everything. I would like to give a special thanks to my best brother Abenezer Abadi for his motivation and enthusiastic to assist me with everything. Shout out of appreciation to my advisor DR. Lemma Lessa, For his time, continuous guidance, patience and Support but Most importantly I'm thankful for his faith in me even when I didn't believing in myself.

I want to offer my kindest gratitude to MR.Yosef Shiferaw from Addis Ababa University's ICT Directorate for his informative comments and questions, which encouraged me to broaden my research from other viewpoints. I'd also want to thank Mr.Gemechis from the Ministry of Health ICT Directorate for his assistance. Furthermore, my heartfelt gratitude goes to Mr. Minen and Mr. Mulugeta from the Ethiopian Public health institute for unwavering aid and insightful comments. My sincere appreciation to MR.Maru who is security department team leader at the information network Security Agency, for his encouragement and assistance. In addition, I'd like to Thank Mr.Yared and Mr. Abraham from ministry of innovation and technology for their tremendous assistance. I'm grateful to Mr. Daniel from Federal Supreme court for the motivation. I wish to extend my gratitude to Mr.Sebsibe and Mr.Turmi from the ministry of Education ICT Directorate for their assistance and constructive guidance. My sincere gratitude goes to Mr.Henok from the Ministry of Revenue ICT Team, as well as Mr.Fasil and Mrs.Abonesh from the Ministry of Transport, for their Assistance. I'd like to thank everyone who scarifies their time to take part in this research.

Table of Contents

List of Tables

List of Figures

List of Acronyms and Abbreviations

CIA	-	Confidentiality, Integrity and Availability
ICT	-	Information Communication Technology
IS	-	Information systems
ISO	-	International Organization for Standardization
ISS	-	Information System Security
ISSM	-	Information system security Management
NIST	-	National institute of standards
PMT	-	Protection Motivation Theory
TAM	-	Technology Acceptance Model
TOE	-	Technological, organizational and Environmental
UTAUT	-	Unified Technology Acceptance Use of Technology
ROSI	-	Return of Security Investment

Abstract

Ethiopian public institutions are investing in various IT infrastructure and systems to improve the effectiveness and efficiency of their operations. Organizations are highly dependent on network connection and information systems which make them to become hot point of cyber-security. With respect to this, the government of Ethiopia adopts a digitization strategy that strength security capacity as a key element. However, most Organizations have hesitated to make security investments due to several reasons. Most organizations do not consider how cyber-attacks affect the costs and benefits, which results in underinvestment in cyber-security. Due to the dearth of information determining the benefit on information security investment (ROSI) is always challenging. Decision-makers are frequently confused by the abundance of competing solutions and unsure of whether their investments in security are appropriate or even effective. The goal of this study is to identify the factors that affect investment in information security based on TOE framework. In addition, the study determines the significance of those factors that affect information system security investment and provide suggestion on how information system security could be guided. Identifying the factors that influence security investment decisions will assist decision-makers to drive better cyber-security investment decision-making in a proper manner. The study used a quantitative research method using questionnaires as a data collection tool. A total of 105 questionnaire sets were distributed, and 86 were returned, which accounts for 81.9% of the total response rate. Descriptive and explanatory analyses were used to examine the data. The result revealed that among organizational factors: management support, economy, awareness, decision support process, risk assessment, future Growth, and organization culture have significant impact on information security investment. Similarly, environmental factors, namely; legal and regulatory framework, have an impact on security investment. Based on the results, information system security investment could be guided by the support and commitment of management. Raising the information system security awareness among management and key decision makers can increase investment in information system security. The greater awareness and support on security among the decision makers, the greater the security investment. Furthermore, Organizations must take risk assessment; create security controls, policies, and frameworks in order to maintain their spending in information security.

*Key words: Information system security, Information system security investment, Technology, Organization, Environmen*t

CHAPTER 1: INTRODUCTION

This chapter will introduce the topic in the broader context and present background information to the research problem. In doing so, it begins with the presentation of Information Communication Technology in organizations, Information security threats, overview of information system security, the essence of information system security information system security in public organizations, information system security investment. The second section focuses on the motivation of the study. The third sector deals with statement of the problem. The sections there after present the basic research questions, the significances of the study, scope of the study, limitations of the study and definitions of important key terms in the study. The chapter concludes by presenting the organization of the paper.

1.1. Background of the Study

With advent of cutting-edge digital technologies, organizations are relying on Information and Communication Technologies (ICTs) to enhance their services and operational effectiveness. ICT has become an integral part of an organization, but they come at a cost. Emerging ICT's create rapidly evolving vulnerabilities that can be exploited by malicious attackers using similarly advancing ways (Wessels *et al.*, 2021). Threats to information security are now evolved in advanced and diverse way. ICT security incident is becoming more sophisticated as companies utilize digital tools to foster innovation (Spremić and Šimunic, 2018).

The enhancement of the digital revolution offers fantastic potential as well as a disastrous retreat from security risks (Lee *et al.,* 2018). Currently, Ethiopia's ICT landscape is drastically evolving. According to ("NCSI::Ranking."2022) Ethiopia is ranked 170th on the ICT development index and 115th on the global cyber security index.

Cyber-attacks can have profound consequences for companies (Carías *et al.,* 2019). Risks that organizations may encounter include data breaches, revenue loss, and attacks on security that has an adverse effect on countries. As (Fedele and Roner, 2022) reported, cyber-attacks may result in significant financial and reputational losses and even jeopardize the ongoing operations of a company, with knock-on effects felt across the entire economy. According to a report by (Aregahegn, 2022) Ethiopia has been the target of approximately 6,000 cyber-

attack attempts in the first 11 months of the current fiscal year and the country has managed to avert 97% of them, saving 1.4 billion birr.

Information system security has a critical importance of safeguarding the assets of organizations. As stated by (Lee *et al.,* 2018) utilizing security technologies is driven more by the desire to reduce harmful threats than by the urge to earn positive benefits. It is crucial to implement efficient information security plan which preserve assets in this critical business environment (Hall *et al.,* 2011).

It is also vital to take some early measures toward gaining a better knowledge of how organizations spend in information security technology as well as how businesses deal with the threat (menace) of breach (Moore *et al.,* 2010). According to (Govender *et al.,* 2018) The entire cost of an organization's security has risen and will keep expanding as a result of the growth in incidents involving information security. To address security risks, a strong transformation plan and deployment architecture that matches with a specific business model for an organization are needed (Venter *et al.,* 2020). The national digital transformation of many countries has cyber-security as its main focus (Armenia *et al.,* 2021). With respect to this, the government of Ethiopia adopts a digitization strategy that encourages the country to go through a digital transformation that considers strengthening security capacity as a key objective (Montes *et al.,* 2023). Ethiopian public institutions are investing in various IT infrastructure and systems to improve the effectiveness and efficiency of their operations. (Digital Ethiopia, 2025) affirms that the digitalization strategy of Ethiopia will help the public sector by enhancing e-government, digital ID, and the national payment system, among other things. Furthermore, one of the missions of Ethiopian ICT policy and strategy is to promote the use of ICT for modernizing the civil and government sector with the goal of optimizing the delivery of services and to promote good governance and decrease wastage of resource (The National ICT policy and strategy, 2017).

According to (Benaroch, 2018) IT investments mainly deal with value-creation while information system security investments concentrate on value-protection. Security investment has played an effective and significant role in curtailing vulnerability and potential damage for organizations (Mazzoccoli and Naldi, 2020). Organizations are highly dependent on network connection and information systems which make them to become hot point of cyber-security (Ng *et al.,* 2013). According to (cybercrimemag, 2019) Due to the exponential rise in cyber-attacks, over the five years from 2017 to 2021, the global investment in cyber security

surpasses $1 trillion. This indicates spending in security is crucial to combat cyber-attacks. This is common for a company to bolster its security systems after breaches happen (Armenia *et al.,* 2021). Investment in security is triggered by a numerous variables practically. There are some challenges on estimating the cost and return of information security investment (Chai *et al.,* 2011). Security has been impacted by a number of elements that are not in the direct control of an individual or an organization (Wessels *et al.,* 2021). In spite of this, the research determines the factors that affect information system security investment using TOE Model to identify the technological, Organizational and environmental Factors. This help decision maker to understand these critical issues and to evaluate when making decision in information security.

1.2. Motivation of the study

Public institutions are making significant investments in information and communication technologies. Both individuals and organizations are very concerned about cyber-security breaches (Gordon *et al.,* 2015). A company can diminish risks and mitigate the effects of cyber-attacks by using the cyber security management model dimensions (Limba *et al.,* 2017). However, putting the best cyber security strategy into practice and investing in cyber security are not simple tasks (Fielder *et al.,* 2018).

Investing in cyber security comes with a variety of difficulties. As stated by (Weishäupl *et al.., 2018*) due to low rate of return and intricate nature of information security controls, organizations downplay its significance and refuse to implement it until they are formally mandated by laws or regulations. As (Gordon *et al.,* 2015) confirms, substantial cyber-security breach was the catalyst for the majority of firms' increasing investment in the field. As specified by (Fedele and Roner, 2022) cost and ongoing uncertainty about the likelihood of security attacks makes security spending less valuable.

According to a study made by (Ng *et al.,* 2013), trust, reputation, and misperceptions about information security were identified as factors influencing SME security investment. The study suggests evaluating additional variables that have an impact on investment of security. A qualitative study made by (Kirubel, 2022) discovered that the key factors affecting information security investments are listed. The researcher advises further research to find other factors that affect security investment as the research only considered Ethiopian-selected banks. By virtue of this, the researcher is persuaded to use the study as a benchmark and broaden the scope into Public organizations using quantitative research design.

The researcher's educational and professional background is directly related to information system, who has worked at different public health institutions. The main responsibility of the researcher has been customizing and managing different health information systems including the national District health information system. This experience has made the researcher notice some problems in public organizations with respect to information security. In the process of deploying organizational information systems, the decision maker has mostly no intention to invest in security solutions. In addition, Decision maker show confusions with regards to investing in information system security. As a researcher worked on different public organizations, mostly, decision makers don't know how and where to invest with regarding to information system security. By considering the above theoretical and practical motivation, the researcher persuaded to study on information system security investment. This research identifies the elements which has an impact on influencing information system security investment and evaluates the significance level of these factors on selected public Institutions in Ethiopia. A deeper knowledge of information system security investment and the factors influencing information system security provided by this study. It raises the level of understanding for decision makers and support organizations in making investment decisions related to information systems security.

1.3. Statement of the problem

The advancement on digital technology allows organizations to increase production abilities, fully satisfy public demand for services and more (Tewamba *et al.,* 2019). Ethiopian digital transformation strategy strengthens the overall digital ecosystem, enables systems, and allows for digital interactions between the public and private sectors (Digital Ethiopia, 2025).

Creating various information systems with a range of functionalities is currently a concern for Public organizations. Although the systems produce good results, there must also be a negative aspect that leaves them highly vulnerable to security threats (Ng *et al.*, 2013). In order to endure cyber risks, it is more appropriate to analyze information security controls to improve through investment (Shao *et al.,* 2019).

Organizations are currently promoting the inclusion of a cyber-security portfolio which safeguards for prevention, detection & containment (Safi, 2016). However, as reported by (Jeong *et al.,* 2019) most Organizations has hesitated to make security investments as they didn't notice seen the anticipated economic damage from security breaches or the anticipated benefit from those investments right away. According to (Chai *et al.,* 2011), due to the dearth

of information for calculating the probability and expense of information security risk factors, determining the benefit on information security investment (ROSI) is always challenging. As (Gordon *et al.* 2015) stated, without additional incentives or regulations, organizations do not consider how cyber-attacks affect the costs and benefits for society as a whole, which results in underinvestment in cyber-security.

Organizations that have experienced a cyber-security incident frequently take action afterward (Wessels *et al.*, 2021). Decision-makers are frequently confused by the abundance of competing solutions and unsure of whether their investments in security are appropriate or even effective (Fenz *et al.*, 2011).

In light of this, this research considers, the TOE framework to investigate the factors affecting information system security investment. In previous IS adoption research, the TOE framework was the most applicable and significant framework (Alwali, 2017). The TOE framework determines the organizational level of innovation adoption by considering technological, organizational and environmental setting of an organization (Tornatzky & Fleischer, 1990). The technology category deals on the advantage of technology with a combination of external and internal value to the enterprise (Alhogail *et al.*, 2015). The organizational context encompasses all aspects of firm, including the structure of the organization, departmentalization, and roles for human resources, level of control, and more (Abed, 2020). Environment refers to the external or inter-organizational setting in which an organization operates (Tornatzky & Fleischer, 1990).

Some studies attempting to shed light on the subject under the study. (Lee *et al.*, 2018) discovered that positive Internal factors, such as assets, experience, facilitation conditions, and habits, have better influence on information security investment than negative external factors, such as threats and vulnerabilities. However, the study used behavioral models and it only focused on the behavioral intention that affects security investment. Thus, it doesn't provide the internal and external factors affecting information system security investment. The study by Toivanen (2015) also examined why information security investment decisions fail, through a various case studies and, the results demonstrated that a variety of factors significantly influence security investment decision-making. However, the finding of the case study doesn't demonstrate the significant level of impact of those factors affecting information security decision making. A study by (Temtim and Alpha, 2021), studies factors that influence employees' compliance with Ethio-telcom's information system security

policy. The survey approach was used to obtain data. As the findings shows, the management support, awareness and trainings and accountability are the major organizational variables that affect employees' behavior in order for them to comply with the existing information system security policy. The study used a single case study and particularly focuses on organizational factors.

A related study made by (Woretaw *et al.,* 2019) analyzed the level of existing information security culture in Ethiopian banking sector using quantitative approach. The findings show that information security knowledge in Ethiopian banking sector is inadequate due to insufficient information security communication and training. The research only emphasis information security culture. (Nebyu, 2018) studies maturity level of information security implementation in Ethiopian public universities sector using Qualitative and Quantitative methods. The finding demonstrates information security control environment in public universities is insufficient and compare the uppermost and lowermost maturity scored information security controls in Ethiopian public universities. The studies only emphasize on the level of maturity of information system security and yet it doesn't prove adequate information on factors that has an effect on the maturity level of information system security. This research provides the TOE factors that has an influence in information system security and provides suggestion on how to improve and guide information security investment in an organization.

(Kirubel, 2022) studies the factors that influence information security in the banking sector, the goal of this study was to identify the factors that can effect investments in information security and to establish a conceptual framework that can help in the selection of security solutions. The author identifies seven variables that can affect security investment through a qualitative case study. The study outcomes demonstrates, the lack of top management support, lack of knowledge and experiences, vendor involvement, lack of budget, lack of assessing risks and vulnerabilities, not considering future growth, and not considering existing infrastructure, lack of knowledge on specific security product, lack of time, lack of well-prepared NBE directives, rules and policies, delayed product delivery period, not considering information security frameworks and standards, and lack of competitive benchmarking. The study only includes Ethiopian banks and is conducted through qualitative analysis. In addition, the research doesn't measure the effect of each factor in information security investment. in order to fill the research gap, this study determine the factors

influencing the investment in information system security using quantitative methods and the scope of the research focused different types of public organizations in Ethiopian Context.

This Research combines multiple theories to identify factors impacting information system security investment using TOE model. Previous studies depend on behavioral models, organizational factors, lack of comprehensive internal and external factors, lack of quantitative statistical analysis which determines how those factors affects information system security investment and lack of assessment of information system security investment in public organizations. By virtue of this research gap, this research identifies technological, organizational and environmental factors impacting information system security investment. In addition, the research also contributes by statically analyzing the significance level of each factor that affects information system security investment and pinpoints important suggestions based on the research findings. Furthermore, this research provides recommendation on information system security investment.

1.4. Research Questions

The following basic questions were developed to guide the study:

1. What are the Technological, organizational, Environmental (TOE) factors influence information security investments in public organizations in Ethiopia?
2. How those factors affect information system security investment in public organization in Ethiopia?
3. How can information system security guided?

1.5. Objective of the study

1.5.1. General Objective of the study

The main objective of the study is to identify the factors Affecting Information System Security investment in Public Organizations using TOE model.

1.5.2. Specific Objectives of the study

Specifically, the objectives of the study are to:

- To identify the Technological characteristics affecting information system security investment

- To explore the Organizational characteristics affecting information system security investment
- To determine the Environmental characteristics affecting information system security investment
- To assess the extent of the impact of Technological, Organizational and Environmental Factors on Information system security investment
- To provide recommendations to improve information security investment in public organizations.
- To provide additional insights on literature about information system security investment this serves as a benchmark for other researches.

1.6. Significance of the Study

The focus of the study is exploring factors affecting information system security in public organizations using TOE model. This study, therefore, has both theoretical and practical significances.

1.6.1. Theoretical Significance

It outlines factors influencing information system security in public organizations, theoretically. The approach, methodology and the scope, to the issue can contribute to the field. This research can be used as a source document for further researchers on this issue.

1.6.2. Practical Significance

The study have a major contribution to elevating the degree of awareness with regard to security investment decision making process and it will provide a clear view of factors that have an influence on the decision-making process with respect to information system security investments. Identifying factors that influence security investment decisions will assist decision makers to drive better cyber-security investment decision-making in a proper manner. According to Safi and Browne (2015), Improving Security decision would be impossible without a thorough knowledge of prospective variables that impacts security investments and budgeting decisions. Finally, the study explained the technological, organizational and environmental factors affecting information system security investment and their significant level of effect on security investment. The findings and recommendations of the study may initiate other researchers in the area to further investigate the issues by considering other variable in relation to information system security investment.

1.7. Scope of the Study

This study addresses the factors affecting information system security investment in selected public institutions. The study used TOE Model which includes the technological, organizational and environmental factors affecting information system security investment in selected Public organizations. To get wider view different types of selected Ethiopian public organizations are included in this study. But due to time constraints, the study's scope area was limited and it includes only Eight Ethiopian public organizations. The purposes of this study are on determining the Technological, Organizational and environmental factors that influence investment in information system security. The primary sources of data are gathered from the organization's employees particularly, ICT senior experts, CIO, CSO, Team leaders, Department head and Directors which is believed they have direct attachment with information system security investment decision.

1.8. Limitation of the Study

There are a few restrictions on this study. There are only eight public organizations and a small population was used. As a result, it cannot be applied to other organizations or nations. This study used TOE Model and asses the technological, organizational and environmental factors only. Other factors are not included in the study.

1.9. Organization of the Study

The study organized under five chapters. The first chapter deals with introduction of the study. It discusses the background of the study, motivations of the study, statement of the problem, objectives of the study, basic research questions, scope of the scope, significance of the study, limitations of the study, operational definitions of the study and organization of the paper. The second chapter deals with the review of the related literature. In doing so, it presents the different studies on information system, information system security, information system security investment, Factors affecting information system security investment and TOE framework. The chapter concludes with presenting the conceptual framework designed to guide the study based on different literatures. The third chapter presents research design and methodology which involves research design, data sources, sample and sampling techniques, data gathering instrument, procedures and method of data analysis. The fourth chapter focuses on presentation, analysis and interpretation of data. The final chapter, chapter five, presents summary of the findings, conclusions, and implications of the study.

1.10. Definition of Terms

This study mainly focuses on Factors affecting information system security investment. The main concepts to be understood here, therefore, are terms like, information systems, information security, information system security investment, TOE Framework are defined as follows.

Information systems: is an interrelated and collaborative group of software-driven information technologies supporting the objectives of an individual, a group, an organization, or society. It facilitates communication and coordination across various functional areas, enables simple data exchange and accessibility across operations, and plays a crucial role in process execution, data collection and storage, and process performance monitoring (Rainer and Prince 2021).

Information system security: the safekeeping of anonymity, authenticity, and accessibility of information by averting against illicit access, use, failure, and harm of information and information systems (Nieles *et al.*, 2017).

Information system security management: it specifies conditions for creating, implementing sustaining, and enhancing management of information security which deploys risk management procedure for safeguarding the privacy, accuracy, and accessibility of data (Al-Dhahri *et al.*, 2017).

Information system security investment: It is a spending in security measures, which helps to reduce security risks (Ng *et al.*, 2013).

Risk: Risk is the chance of exposing company's information and communications systems to potentially harmful people, things, or circumstances that could result in loss or damage. Risk denotes a level of probability or the likelihood that an event will occur. (Zimmermann, *et al*., 2019).

Vulnerability: is a defect in a system, security method, internal controls, or deployment that a threat source could exploit, which could cause large and occasionally irreparable damage to an individual, group, or organization (Avci and Ozbulut, 2018).

Threats: is anything that has the potential to jeopardize the safety, security and accessibility of information, or to harm others sorts of information system resource (Geric *et al.*, 2007).

Confidentiality: protection against the misuse or disclosure of information assets (Oscarson, 2003).

Integrity: the information sources shouldn't ever be modified or altered by an unauthorized party (Srinivas *et al.,* 2019).

Availability: It focuses on only those who are permitted should have access to the resources they require to do their jobs (Nweke, 2017).

TOE framework: is a model that adequately describes the organizational situations in which new technology taken up and utilized from the organizations perspective (Tornatzky & Fleischer 1990). It depicts the elements that impact the process by which organizations embrace information technology which are classified into technological, organizational and environmental factors (Kim and Kim 2021).

CHAPTER 2: LITERATURE REVIEW

The purpose of this chapter is to present related literature to provide understanding on the information system security investment decisions. The chapter consists of the following major topics of: introduction to information system, information systems security, information security management, major information systems assets, Major threats and vulnerabilities in information security assets, information system security controls, Information systems security in public organizations, Information system security risk management in public organizations, information technology investment, Information systems security investment, factors affecting Information systems security investment in public organizations, The Technology organization and Environment framework and review of related works and conceptual framework.

2.1. Information System

An information system (IS) means the collection of interconnected parts which gathers, manipulates, stores, and disseminates data and information as well as offers a feedback mechanism to achieve a goal (Stair and Reynolds, 2020). With respect to (Laudon and Laudon, 2004) stated, Information systems are a combination of process that provide for acquiring, modifying, and transmitting information that may utilize to better organizational performance.

Organizations have driven up their operations of using information technology (IT) in order to enhance cooperate operations and decision making process (Chu *et al.,* 2020). The accelerated process of information used by companies on a regular basis to fulfill their goal of meeting the demands of stakeholders and adjusting to their environment (Tewamba *et al.,* 2019). Information system has become an important tool in public organizations to improve efficiency of internal operations and the relationship with customers. Many organizations today have accelerated and hurried to locate, create, and profit from such systems in order to fulfill their goals. However, the advancement of the digitalization can lead to both huge opportunities and catastrophic disasters (Lee *et al.,* 2018). As the system expands, ensuring information security and preserving important business assets become more difficult (Lavrov *et al.,* 2021).

Organizations typically unable to safeguard their assets because they depend on insufficient and inappropriate technology solutions (Khando *et al.,* 2021). Organizations are susceptible

to cyber risk, which increase the possibility that the private information provided to them may be violated, lost or exposed (Kamiya *et al.,* 2021). Cybercriminals are utilizing new strategies, exposing more data, and having a greater negative impact, which has both direct (on business operations and money trails) and indirect financial repercussions (stolen identity, lost privacy, reputation etc.) (Spremić and Šimunic, 2018). The rises in cybercrime expose firms to greater information risk, and distract organizations from regular activities which could have serious consequences in the organization (Carias *et al.,* 2019). These effects are going to affect the company's reputation and operational performance. Aside from that; Dramatic changes in organizational architecture, data management systems, technological ramifications, issues are only a few of the new difficulties it has brought along (Soomro *et al.,* 2016). Given the increasing frequency of cyber-attacks that result in crucial costs to businesses and individuals, cyber-security becomes major essential elements of risk management for organizations (Lee *et al.,* 2018). As (Verbano and Venturini, 2013) discussed, to survive in the market, organizations must have an information system security and risk management strategy to recognize, determine and mitigate threats. According to (Kim and Kim, 2021) stated, Information security is getting more attention as organizational activity increasingly depends on technology.

2.2. Information systems security

Information systems security is defined as sustaining the system privacy, reliability and accessibility (Ioannidis *et al.,* 2016). The major purpose of information system security is to safeguard the integrity, availability and confidentiality requirements for security objects are not jeopardized (Lundgren and Möller, 2017). Secured information is said to have integrity if only authorized user can alter. Information integrity can be achieved through the use of encryption, access for user, backup and recovery protocols (Olsina *et al.,* 2014). Confidentiality deals on if only authorized users can view it. According to (Jabangwe and Nguyen, 2020) Confidentiality can be attained through encryptions, password, two-factor authentication and biometric verification (Qadir and Quadri, 2016). Availability Ensure that authorized users can access and use data on demand such that Access to the system. Availability focuses on if only authorized users may access it whenever they need it (Kim and Kim, 2021).

Information security is one of the most important aspects of organization security management which preserve the assets in an organization (Ključnikov *et al.,* 2019). Public

sector companies prioritize serving individuals with a social mission and focus on welfare of the community. However, while they go about their mission, they have to deal with several threats, both internally and externally (Patino and Yoo, 2018). Organizational activities are hampered by the organization's concern for information security management (Alhogail *et al.,* 2015). While much of attention on information security is on technical issues, employees in organizations are major flaw in securing information assets. According to (Cheng *et al.,* 2013) people play a vital role in information security. They could be the weakest link. Information security cannot be achieved solely through the use of technology but rather through the employment of three components these are peoples, process and technology (Ifinedo, 2013). As (Siponen *et al.,* 2014) stated, the major threat to information security is the information system user. Therefore, the organization must choose appropriate preventive measures and actively address threats in order to develop a mature ISRM.

2.3. Information security management system

It is one of major component of the company, with the aim of creating, enforcing, supervising, reviewing, maintaining, and improving information security in the organization (Rajnoha *et al.,* 2017). An ISM entails integration and collaboration of business and information security policies, creation of an organization's information security policy, and decision-making about personnel management and handling in the organization (ISO/IEC 27001, 2013). With respect to (Davidavičienė *et al.,* 2019) the primary objectives of information security management are to setup, carryout, monitor and evaluate information security in the organization. As (Ključnikov *et al.,* 2019) stated, The most crucial component of information security management success is the establishment of security controls, which Encompasses technological and procedural information security controls, managing risks and standard application as well as top management support. In accordance with (Carías *et al.,* 2019) stated, the top management's support and awareness are proven to be the most important elements in determining the effectiveness of ISMS. With relates to (Soomro *et al.,* 2016) emphasize the role of management in information security management. Top management support is an essential element of effective information security management (Kazemi, 2012). Top management can assist information security in a number of ways, such as by allocating funds and resources and highlighting how important security is for other aspects of the organization (Kayworth and Whitten, 2010).

According to (Tu *et al.,* 2018) emphasized on the analysis of factors that influence information security management success. The author identified six crucial components for success. The authors' conclusion was that alignment of business, support from organization, IT competencies on IT, and organizational awareness on security threats and controls may all help establish information security controls successfully. The defined variable has an impact on information security, and sophisticated solutions often integrate all of them. According to (Kazemi, 2012) confirmed, the successful implementation of information security management depends on several factors , including management assistance, employee responsibility and commitment, education and trainings, information security regulations, international standards, and the employment of outside consultants.

2.4. Major information systems assets

Information system assets include computer hardware, network devices, and other IT infrastructure, as well as the data and information contained there-in (Safi, 2016). Information has become one of a company's most crucial competitive advantages and a high-value in-tangible asset (Ključnikov, 2019) and (Safa *et al.,* 2019).

Securing information system assets has become a top priority for organizations in the emerging digital world with the goal of protecting them from malicious harmful attacks (Khando *et al.,* 2021). New hazards to the security of information assets are constantly being introduced by the quick advancements in information technology and systems (ICT). Information assets should be treated carefully by a custom security because they are the cornerstone of all information systems (IS) (Tewamba *et al.,* 2019).

The protection of information systems assets is given by cyber security, which prevents unauthorized access by adversaries (intruders or attackers), as well as damage or misuse of the systems' data, hardware, software, and related infrastructure (Srinivas *et al.,* 2019). In order to survive in this extremely fiercely competitive climate, Organizations are increasingly focusing on information security management as a key strategy for managing and effectively safeguarding their digital assets (Hashim and Razali, 2019). Knowing which information assets are significant to the company, locating, classifying, and recognizing those assets, as well as being aware of how they are currently secured, are all necessary (Whitman and Mattord, 2012).

Security professionals should prioritize resources to safeguard valuable assets and pay attention on the users most likely to cause trouble (Sarkar, 2010). An organization must examine how technologies employed and what the threats and vulnerabilities exist in the organization (Lee, 2021). According to (Safi, 2016), Information asset security can be seen as a series of steps or a continuous process. A number of conceptually and operationally distinct but interrelated steps can be used to break down these process interdependent steps. The main steps in securing information assets: prevention, detection, and response.

Prevention*:* The goal of prevention is to lessen the system's susceptibility to dangers, in addition reduce the occurrence of successful accidents. There are several techniques to decrease the likelihood of threats (Safi, 2016).

Detection: is the act of detecting hazards that evade the preventive measures on given time. (Safi, 2016).

2.5. Major threats and vulnerabilities in information security assets

Computers and information technology (ICT) are swiftly evolving, presenting new vulnerabilities to information assets. Currently, the usage of ICT make information security crime easier, an in certain case undetected (Alhogail *et al.*, 2015). Organizations are vulnerable to some level of danger and some attacks are effective (Kamiya *et al.*, 2021). Based on this, Organizations must improve information security capabilities to react effectively survive in this highly Risk environment. As (Fielder *et al.*, 2016) stated, each organization must take into account the dangers from which they are most vulnerable and take steps to minimize their exposure to as many pertinent vulnerabilities as they can (lee *et al.*, 2018).

Most organizations' computer systems are much less safe than they ought to be, thereby making them more vulnerable to cyber-attacks. According to (Abomhara and Koien, 2015), stated, technical vulnerability includes absence of skill and knowledge, inadequate resource, lack of proper project planning, a lack of awareness of user demands, and the inability to manage and control the system development process. A digital infection is one method of exploiting information system security. A digital infection that poses a risk to computer users includes Trojan Horses, Worms, and viruses etc. (Tasril *et al.*, 2017). The major information system security threats are listed as follows:-

i. Phishing Attack

It is a type of social engineering, it entails duping a person into accessing a phoney website by persuading them to click on a certain link (Srinivas, 2019). The type of cyber assault is commonly successful due to user ignorance of vulnerabilities or inability to detect the risks. (Desolda et al., 2021).

ii. Social engineering

It is involve on manipulating someone with the ability to grant or facilitate access to a system or data. Following that, a social engineer can use information-gathering strategies including dumpster diving, desktop spying, shoulder surfing, or CD/USB dropping (Sarkar, 2010).

iii. Identity Theft

It is the act which id secretly obtaining other person's financial or personal information in order to carry out covert, criminal operations (Kirubel, 2022).

iv. Worm

Computer software that is able to replicate itself on a system without requiring authorization (Tasril *et al.*, 2017). Some worms (referred to as "body less" or "package" worms") spread via network packages, enter the computer's memory, and deploy their code there (Lavrov *et al.*, 2021).

v. Ransom ware:

It is malware that restricts or prohibits users from accessing their IT infrastructure systems by doing unauthorized activities such as like locking the system's until a specified or unless a required fee (ransom) is paid. (Srinivas, 2019).

vi. Trojan horse

It appears to be beneficial or useful but it conducts a range of functions without the user's knowledge including acquiring sensitive data, transferring it to an attacker, as well as erasing and maliciously modifying information (Lavrov *et al.*, 2021).

vii. Spyware

A program which has the ability to covertly record all computer network activities. PINs, passwords, bank accounts, and other information are among the things it can steal. The recorded information will be delivered to the malware creator (Tasril *et al.*, 2017).

2.6. Information system security controls

The ability of organizations to defend themselves from prospective cyber-attacks is one of the main problems they are now facing. Organizations must prioritize their defensive strategies due to the breadth and depth of these unidentified attacks (Fielder *et al.*, 2018). The most crucial element in information security management success is security controls (lee, 2021).

Despite the rapid growth of computer facilities and information technologies, current information systems' and computer networks' susceptibility to attack remains high (Lavrov *et al.*, 2021). The achievement of information security management is proved by the results of technical and procedural information security controls, risk management, and implementation of guidelines (Ključnikov *et al.*, 2019). Organizations need to establish thorough security preventative measures that protect the security of information at all information management levels (Temtim and Alpha, 2021). Some organizations spend millions in creating robust perimeter defenses to safeguard their crucial infrastructure and data from outside hackers and attacks (Sarkar, 2010). The major information system security controls are presented in table 2.1.

Table 2.1: Major Information System Security Controls

Security Control	Description
Anti-virus software	An antivirus program is a software application that scans a computer for malicious software, such as viruses and worms, and takes steps to prevent, stop, and remove it (Reddy and Reddy, 2014).
Firewall	Firewalls are set up to only let certain types of traffic in and out (Sarkar, 2010).
Audit Logs	To give a comprehensive picture of network activity, audit logs from numerous sources, including firewalls, intrusion detection systems, intrusion prevention systems, and software and hardware applications, must be merged (Sarkar, 2010).
Encryption	The information stored on the servers must be encrypted in order to prevent a potential adversary from accessing it without the secret key (Srinivas, 2019).
Awareness	It is critical component for ensuring information security and

	protecting an organization's assets from attacks (ISA) (Khando, 2021). Users and employees must be aware of potential hazards like phishing, malware and harmful file downloads, (Srinivas, 2019).
Intrusion detection and prevention systems	It is a security tool which continuously scans host besides network traffic for any unusual activity that might be in violation of the security policy and jeopardize its confidentiality, integrity and availability (Ng *et al.*, 2021).

Source: Literature Review, 2023

2.7. Information systems security in public organizations

Government and private sectors organizations are relying on information technology in support their objectives and business missions (Getnet, 2020). Several public organizations around the world utilize and depend on digitally-enabled government services (Khando, 2021). Rapid digital capability, innovation, and IT skill integration is now a crucial national practice in the overall community development and national economy. In addition, as software evolves and becomes more complex, the quantity of malicious software increases, and the interactions that result in the execution of such threats are quite complicated (Lavrov *et al.*, 2021). Therefore, it is now essential for organizations to employ information system security measures. Public organizations must be able to properly foresee and manage risks as a result (Patino and Yoo, 2018).

ISA is necessary to guarantee that the CIA has access to the vital information stored in the e-government systems (Khando, 2021). Due to this, organizations should increase their information protection spending in order to handle IT disaster recovery, incidents of security, other pertinent issues using an information security management system (ISMS) (Kim and Kim, 2021). Most fundamental security functions are installing firewalls, antivirus programs, and encryption technologies protects organizations' digital resources from cyber-attacks and intrusions; however it is insufficient to address modern cyber-security needs (Lee, 2021).

2.8. Information system security risk management in public organizations

The term "risk management" refers as a formalized method for discovering, assessing, and choosing management approaches to risks. Any risk can be reduced by lowering the possibility of its occurrence through ongoing control over and observation of occurrence

conditions, as well as by reinforcing vulnerability points; shifted from one danger to another (Samimi, 2020).

The first step in managing insider threats is to recognize their existence. Insider risk cannot be managed just through technology means; organizational strategies and human resources must be employed simultaneously (Sarkar, 2010). According to (Lee, 2021) stated, Technical and human factors must both be addressed holistically in cyber risk management. The employment of technological and non-technical controls as well as best practices in information security and governance is required to optimize adequate protection (Nicho, 2018).

The basis for risk analysis is the chance of an event occurring with respect to the consequences it will have. The occurrence is based on the possibility that the risk will occur and how infrequently it will do so (Alali *et al.,* 2018). According to (Lee *et al*, 2018) stated, the most common risk assessment divides risks into two parts: (1) the likelihood that a risk will occur and (2) the potential impact. These two parts are then multiplied to determine the scale of the risk (De Vries, 2017). Security functions can focus their efforts (and corresponding investments) where they bring the most value by being aware of the pertinent dangers to their industry in general and to their organization specifically, right down to the level of business units (Schatz and Bashroush, 2018).

2.9. Information Technology Investment

As (Bacon, 1994) deals that any spending that considers the more than long term capital investment for information technology purposes. When an organization selects how to safeguard its network, it must usually consider two crucial factors: the cost of deploying a specific defense and the impact that defense will have on the business (Fielder *et al.,* 2016).

The fiscal basis of information security expenditure is a fundamental issue for information technology management (Toivanen, 2015). Information technology investments make up a sizable portion of organizations' expenditures, therefore managers must comprehend the expected effects and mechanisms in order to decide and maximize the value of their information technology and related resource allocation processes (Mithas *et al.,* 2012).

2.10. Information system Security investment

Information system security investment is a spending in a security related operations. Security investment is relates to establishing security with a particular focus on the

investments in prevention, detection and response in an expansion in overall security expenditure (Safi, 2016). As (Wang, 2019) describes, spending in technology and tools and Spending in knowledge and expertise are two kinds of security investment. This can include investing in cyber security hardware and software, as well as employee training, as well as changing organizational operations that may increase day-to-day running costs by limiting how IT systems can be installed or how users can access/interact with IT systems (Rowe *et al.*, 2006).

According to (Liu *et al.* 2011) stated, Investments in information security are a direct means to enhance a company's security and should be undertaken after seriously balancing the expenses of the investment with the gain in security that is provided by the investment. Thus, Investments in information security reduce organizational risks (Lee *et al.*, 2018). As (De Vries, 2021) stated, With the increase of the number of cyber-attacks organizations can face serious losses and need to consider investing in their security, how much they should invest and on what measures. According to (Safi and Browne, 2015) discussed, the quantity invested in securities, like any other investment, may be insufficient, adequate, or even excessive depending on the situation. As (Toivanen, 2015) indicates, Information security investments made properly can enhance and improve corporate performance. However, most organizations are hesitated to invest in information security (Jeong *et al.*, 2019).

Information security managers must use good decision-making techniques when investing in cyber security resources (Fielder, 2016). With respect to (Safi, 2016) stated, even when security investment is successful, decision-makers may not have adequate motivation to keep investing in security because there are frequently no indicators that a danger has been properly neutralized.

It was discovered that the domain of security investment as it relates to structuring security solutions emphasizing the fact that investment can be made in both prevention and in detection and response as a result of this, the overall security expenditure increases (Safi, 2016). Organizational investments in information security, such as the expense of solutions,, the amount of cost of paying professionals, the expense of an external security assessment, etc., are gradually rising from every year but frequently are ineffective (Lavrov et al., 2021). With respect to this, Security investments must be carefully calculated to achieve the demand of the business (Mazzoccoli and Naldi 2021).

The investments made in security solutions are impacted by a variety of factors. One of the important drivers included the threat landscape, legal and regulatory frameworks, and risk frameworks (Schatz and Bashroush 2018). When deciding on additional security investments, organizations must consider their financial capacity, top management commitment and understanding of cyber security, the level of skill and knowledge of their cyber-security team, external pressure from vendors, and past activities (Weishäupl et al., 2018).

2.11. Empirical Review

As far as the researcher's knowledge, there is no study exists that identifies factors influencing Information system security investments in selected public organization using TOE Framework, In case of Ethiopian Context. However, there are several studies conducted in factors affecting information system security investment. These related works of literatures are discussed below.

(De Vries, 2017) conducted a study focused on factors respect to organizational context which impacts investment strategies and to find individual perspectives from decision-makers regarding cyber security investments. The study analyzed investment strategies in the first place and organizational factors that influence these strategies and personal perspectives that influence the investment strategies. However, the study only focuses on organizational factors and some variables were not clear or not correctly categorized. In addition, the effect of this factor stays unknown in this study. Based on the gap discussed, this study aims to fill the research gap by focusing on determining technological, organizational and environmental variables which affect information system security investment. The outcome demonstrates the significant degree of influence of such variables on information system security investment.

According to (Ng *et al.,* 2013) conducted a study on factors affecting information system security investment. The study has identified three key motivating factors from a series of case studies. Trust, reputation, and a misunderstanding of information security have already been identified as factors impacting SMEs in this study; they are only helpful in giving us insights into the decision-making process. The survey only covers small to medium-sized businesses. But according to this study, there are technological, organizational, and environmental factors assessed that have an influence on information system security investment. In addition, statistical analysis has made to find out the level of effect of each factor on information system security investment.

A Study by (lee *et al.*, 2018) examines elements that impact information security investment and to provide policies for improving information security through information security investment in fourth industrial revolution. This study designed a research model for information security investment variable based on the information security risk management, protection motivation theory, UTAUT and empirical data were analyzed by structural equation analysis with statistical program, The results demonstrates, that information assets, facilitation conditions have a high significance effect influence on experience and habits, intention to investments and experience and habits, investment intention have a strong influence on the 4th Industrial Revolution . The research gap shows, the study is limited to behavioral models which is UTAT and protection model which doesn't include other model which encompasses internal and external factors that affect information system security investment. Therefore, this research presents internal and external factors and provides the significance level of each factor that affects information system security investment.

A study by (Safi, 2016) investigates investment behaviors in the domain of information security through experiment comprised of a series of novel economic games. It determines empirically how efficient human decision makers are in allocating monetary resource to security when the key attributes of the risk environment as well as the key attribute of the available risk mitigating measures are known. The other goal of the study was to determine, how a specific security budget is allocated to preventive and response methods as two major kinds of security practices, the study findings shows, decision makers tend to respond to minor security concerns by investing in security when no security investment is economically justified. In addition, the possible behavioral biases influence information security investment decision. The study only determines the behavioral factors which impacts information security investment, it doesn't asses other technological, organizational and environmental factors which impacts investment in the domain of information security.

A related study made by (Woretaw *et al.*, 2019) analyzed the level of existing information security culture in Ethiopian banking sector using quantitative approach. The findings show that information security knowledge in Ethiopian banking sector is inadequate due to insufficient information security communication and training. The research only emphasis on information security culture. With respect to (Nebyu, 2018) studies maturity level of information security implementation in Ethiopian public universities sector using Qualitative and Quantitative methods. The finding demonstrates information security control environment in public universities is insufficient and compare the uppermost and lowermost

maturity scored information security controls in Ethiopian public universities. The studies only emphasize on the level of maturity of information system security and yet it doesn't prove adequate information on factors that has an effect on the maturity level of information system security. This research provides the TOE factors that has an influence in information system security and provides suggestion on how to improve and guide information security investment in an organization.

A study by (Temtim and Alpha, 2021), studies factors that influence employees' compliance with Ethio-telcom's information system security policy. The survey approach was used to obtain data. As the findings shows, the management support, awareness and trainings and accountability are the major organizational variables that affect employees' behavior in order for them to comply with the existing information system security policy. The study use a single case study and particularly focuses on organizational factors. It doesn't provide internal and external factors that influence employees' compliance. (Kirubel, 2022) studies the factors that influence information security in the banking sector, the goal of this study was to identify the factors that can effect investments in information security and to establish a conceptual framework that can help in the selection of security solutions. The author identifies seven variables that can affect security investment through a qualitative case study. The study outcomes demonstrates, the lack of top management support, lack of knowledge and experiences, vendor involvement, lack of budget, lack of assessing risks and vulnerabilities, not considering future growth, and not considering existing infrastructure, lack of knowledge on specific security product, lack of time, lack of well-prepared NBE directives, rules and policies, delayed product delivery period, not considering information security frameworks and standards, and lack of competitive benchmarking. The study only includes Ethiopian banks and is conducted through qualitative analysis. In addition, the research doesn't measure the effect of each factor in information security investment. in order to fill the research gap, this study determine the factors influencing the investment in information system security using quantitative methods and the scope of the research focused different types of public organizations in Ethiopian Context.

2.12. TOE FRAMEWORK

The technology acceptance model (TAM), protection motivation theory and the unified theory of acceptance and use of technology (UTAUT) are significant theories that are used to explain how innovations are adopted by enterprises (Bryan and Zuva, 2021). The TOE

suggested by (Tornatzky et al., 1990) is used by a variety of previous studies to comprehend how adoption of innovations develops on the organization (Abed, 2020). The TOE framework is significant model used in the previous IS/IT adoption studies. (Alwali, 2017). Its advantage over other behavior models is that it reflects how different factors (both internal and external) affect adoption decisions based on the following three contextual groups: technology, organization, and environment (Kim and Kim 2021). The TOE model effectively determines the organizational situation where new technology is adopted and deployed from the organization's perspective.

Technology Context

The technology category deals on the advantage of technology with a combination of external and internal value to the enterprise (Tornatzky & Fleischer, 1990). According to (Obeidat & Mughaid 2019) indicated that Security tool suppliers fail to emphasize that over time, these solutions must be upgraded to counter new threats and attacks; as a result, systems in an organization are left open to new dangers.

Organizational Context

(Tornatzky & Fleischer, 1990) explains the organizational context refers to the qualities and resources of organizations that either help or impede the adoption of technological innovations, and it represents the intra organizational environment. The organizational context encompasses all aspects of firm, including the structure of the organization, departmentalization, and roles for human resources, level of control, and more (Abed, 2020).The decision to make an investment in information security is significantly influenced by the organizational setting. This includes the processes used to make decisions, the restrictions placed on the CISO, the important stakeholders, (Dor and Elovici, 2016). According to (De Vries, 2021) organizational investment strategy is highly affected by the size and revenue of the organization.

Environment Context

Environment refers to the external or inter-organizational setting in which an organization operates (Tornatzky & Fleischer, 1990). Information security benefits to an organization are greatly influenced by aspects connected to the business environment, especially strategy, goals, and culture etc. (Schatz and Bashroush, 2018). According to (Dior and Elovici, 2016) The supervision of governmental regulatory occurs in the external environment of the

business, influences the organization's decision-making process. The foundation on which security investment decisions are based is the business environment. Without properly taking it into account of environment, security programs won't be useful. (Schatz and Bashroush, 2018).

Environmental factors have both direct and indirect effects. Suppliers, workers, laws and regulatory bodies, consumers, and rivals are all direct effect factors on the organization's operations. Indirect impact factors may not have a direct or immediate impact on the organization's operations, but they may have an impact (Bryan and Zuva, 2021).

In light of the Study objectives, fourteen(14) factors adapted from the TOE framework and identified as relevant under three characteristics: Technology context, organizational context, environmental context. In terms of Technological context of the toe framework, determines the quality of information system solution. The organizational context of TOE identifies the Top management Support, misperception of ISS, Economy, Awareness, Risk assessment, Decision support process, consideration of organization infrastructure ,Consideration of future growth and organization culture,. Moreover, The TOE framework's Environmental Context investigates the legal and regulatory framework, Vendor Involvement, security incident and financial model.

2.13. Conceptual Framework

2.13.1 Factors Affecting Information System Security

Organizations must spend in cyber security activities to keep themselves against the negative effects of cyber security breaches (Gordon *et al.,* 2015). There are different factors which affects information system security investment. It is crucial to understand the organization's top priorities when making an investment choice involving information security (Toivanen, 2015). There are numerous factors affecting information system security investment.

i. Quality Information system security

A systems quality refers to an aspect of the system such as reliability, adaptability, ease of use and functionality (Tewamba *et al.,* 2019). According to (Charlton and Cornwell, 2019), the level of compatibility between new technology or innovation and current technology shows the compatibility assumption. For cyber security technologies to be adopted, compatibility is crucial issue (Hasani *et al.,* 2023). On the basis of the technology's on-going

appeal and efficacy, prospective adopters of technology assess the effects of their adoption actions (Caffaro *et al.,* 2020). According to (lee *et al.,* 2018) stated, the quality of security technologies has an effect on the intention to utilize and invest in information security technology. As (Tewamaba *et al.,* 2019) discusses the quality of security solution determines by its flexibility, ease of use and functionality. The degree to which a new technology is accepted is influenced by its level of complexity (Laurell *et al.,* 2019). Individuals can test if an element of technology works well in their setting because of trialability, which has a big impact on adoption (Hasani *et al.,* 2023). According to (Weishäupl *et al.,* 2018) discussed, due to the lack of return and complexity of information security controls, organizations downplay its significance and refuse to implement it until they are formally mandated by laws or regulations. The ideal degree of cyber security expenditure is determined by criteria such as the compatibility of available cyber security technologies with current technologies, as well as the security requirements of the products and services offered by the firm (Rowe *et al.,* 2006). Therefore, Based on the evidences presented above:-

H_1: Quality of information system security has significant effect on information system security investment.

ii. Management Support

According to (ISO 27002) the support and participation of top executives is necessary for implementation of an information security. According to (Temtim and Alpha, 2021), Management support refers to the actions, spending and activities taken to implement information security norms throughout the institutions. Management determines security priorities and investment resources based on overall business operations (Rowe et al., 2006). A good management review should seek for methods to improve (Hashim and Razali 2019). Management plays an important role in resource allocation decisions on the firm (Gordon et al. 2015).

Organization effort to promote ISS effectiveness such as reward and bonuses and may provide an external motivation for organizational members to follow ISS policies and practices (Alhogail, 2015). As (Aghaunor and Okojie, 2022) discussed, Management should monitor compliance to the organization's rules, procedures, and behavioural regulations. This is crucial since it has the ability to reduce risk by safeguarding the organization's IT resources. The main barriers for public organizations and small medium size business faced

are to hire security professionals due to Low-level security of the organization (Lee et al. 2018). (Hashim and Razali, 2019) stated, top management is responsible for directing the organization and cooperating the activities to achieve that the ISM objectives are met. Management, leadership, accountability for information security in the organization are all critical building blocks for instilling a robust information security culture (De Vries, 2017).

Top management can further demonstrate responsibility for cyber security performance by participating directly in all internal talks about cyber security and by pledging to support any cyber security initiatives. Finally, top management needs to present a future vision for the company's cyber security approach. (Hasani *et al.,* 2023). In General, organization top level management support has the greatest impact on information security (Ključnikov *et al.,* 2019). Therefore, Based on the evidences presented above:-

H_1: Management Support has significant effect on information system security investment.

iii. Misperception Towards ISSI

Misperception of information security is a misunderstanding or false notion negative attitude on information system security (Ng *et al,* 2013). Misconceptions about incidents on security can have a negative impact on an organization's decision to invest in information security in a variety of ways. Lack of specific information and expertise might lead to incorrect judgments (Khando, 2021).Organizations continue to focus on external dangers such as viruses while consistently underestimating the severity of internal issues (Lavrov *et al.,* 2021).

In addition, security practices are seen as having a burdensome and time consuming activity. (Lavrov *et al.* 2021).Furthmore, security practises are seen time consuming and reduce organization productivity and operation (Dor and Elovici, 2016). Organizations believe that security difficulties are solely arising by external forces, and they believe that they cannot prevent predetermined attacks because they don’t understand the benefits of information security (Ng *et al,* 2013). Training provides users with the tools and knowledge they need to implement information security within their organizations (Alqahtani, 2017). SETA is applied to assist employees in understanding information risk and threats, what and how to establish information security controls, and how to comply with information security policies, procedures, and relevant standards (Da Veiga *et al.,* 2020) Therefore, Based on the evidences presented above:-

H_1: Misperception has significant effect on information system security investment.

iv. Economy

Economy is the finical ability of organization to invest in information security. According to Investment on security is the entire amount allocated to it in an organization's budget. This entails allocating funds to various risk management alternatives (mitigation, avoidance, transfer, and retention) and security investment strategies (proactive versus reactive, technological versus organizational, etc.). The price of personal safety precautions is even more specific (Böhme, 2010).

Organizations are not required to increase their budget if the organization's information system damages are small or nonexistent (De Vries, 2017). Accurate cost and effectiveness measurements of an organization's information security efforts are frequently challenging, because security is often an investment that prevents loss rather than one that generates profit, Economical, particularly budgetary, decisions on security investment are challenging. This is a complex procedure due to various issues, including the challenges of assessing returns on investments in security and characterizing uncertainty of these returns. As (Lee *et al.,* 2018) discusses, the high facilitation, the greater the investment. Therefore, Based on the evidences presented above:-

H_1: Economy has significant effect on information system security investment.

v. Awareness

Security Awareness is knowledge on information system security, According to (NIST special publications 800-16) awareness has an objective of allow individuals to draw attention or recognition on Information security concerns. According to (Fenz et al., 2011), one key reason for ineffective or risk management techniques is a dearth of information security awareness at the decision makers and management. According to (Kagwiria, 2020) stated, Decision makers lack confidence in their technicians' Information Security skills and understanding to deal with new security concerns. Furthermore, most organizations are unwilling to fund their employees for professional certificates (Fields and Patrick, 2016).

Most information system security decisions are taken without considering the likelihood of occurrence, the likelihood of outcomes, or the repercussions. Lack of specific information

and expertise can lead to poor judgments (Desolda *et al.,* 2021). According to (Kirubel, 2022), the security team's various educational experiences, skills, and experiences have a considerable influence on the security investment decision. Regarding the organization's level of information security maturity, it is crucial to take user roles and their skills into account. In an organizational setting, user knowledge of the environment is crucial. This knowledge should be both technical in terms of understanding technical assets and institutional in terms of being aware of security regulations (Maarop *et al.,* 2015). Awareness on information security solutions, as well as routine security vulnerability checks, has a beneficial influence on security investment (Lee *et al.,* 2018). An average information technology user is not necessarily technically educated, and has most certainly not studied cyber security in his or her prior education (Kljucnikov *et al.,* 2019). As a result, in order to strengthen information security, it is vital to promote the usage of security services and product. Therefore, Based on the evidences presented above:-

H_1: Awareness has significant effect on information system security investment.

vi. Organization information security culture

According to (Weishäupl *et al.,* 2018), the absence a robust security agenda has an influence on investment with regard to security (Toivanen, 2015). According to (Brock and Khan, 2017), the neglect of the organization to establish the proper security culture has led to a rise in security threats associated with information systems. According to (Alhogail *et al.,* 2015), the organization's management is responsible for developing the proper security culture and incorporating it into the long-term agenda. It may be advantageous to develop further links between senior management involvement in fostering an information security culture includes strategic management and planning, organizational communication, managerial and operational oversight, and led to have a desired information security decision making (Parsons *et al.,* 2015). Other ways for managers to encourage employees include idealizing security influence in an organization, giving each person special attention, and inspiring drive (Choi *et al.,* 2018). At all levels, the information security program plan should be applied across the whole organization. Information systems are only secure when security technologies and policies are properly integrated, and then employees fully and firmly embrace these policies resulting in compliant behaviour. (Choi *et al.,* 2018).The IT and business teams should collaborate, effectively coordinate, and explain the risks and mitigation methods in addition to sharing common duties. The management of the

information security program ought to be a cooperative effort between business and IT. Together, the business and IT leaders should create the governance frameworks to ensure seamless (Edwards, 2018). Therefore, Based on the evidences presented above:-

H_1: Organization Information Security Culture has significant effect on information system security investment.

vii. Risk Assessment

It is the process of determining, analyzing and evaluating risks in order to prevent security flaws and vulnerabilities (De Vries, 2017). According to (Ernest *et al.,* 2006), the organization's risk management framework should fully integrate the information risk assessment and mitigation policies and processes with the strategic business-level risk analysis and management. The entire decision-making process of cyber risk management decision making process can influence a choice, but organizations can also merely only focus on a certain aspects of risk management, this has an effect on investment decision regarding to security investment (Klijucnikov, 2019). The previous user experience and periodic information security inspection has advantage to implement security solutions (Lee *et al.,* 2018).Therefore, Based on the evidences presented above:-

H_1: Risk Assessment has significant effect on information system security investment.

viii. considering the existing organization infrastructure

It is determining the compatibility of existing organizational environment while incorporating with new solutions. The organization infrastructure consists of technological and non-technical assets of the organization. According to (Toivanen, 2015) Organizational decision makers should emphasis on the compatibility of information security investments with the organizational environment and their usefulness to the organization. Before adopting and implementing security solution, it's preferable to consider the existing organizational structure compatibility (Eric 2018). It is critical to communicate to stakeholders, that information security investment does not require the users learn new technical skills and its implementation is as harmless as possible for users (Toivanen, 2015). Flexibility has frequently been seen as being demonstrated by a person's ability to deal with, adapt to, and recover from a terrible event (Riolli and Savicki 2003). In making an investment decision, a manager can imitate others. Even if the option proves to be inefficient, the manager is not

alone in making the wrong decision and so bears responsibility alongside those who accepted or refused an efficient information security investment (Shao *et al.*, 2019). Countermeasures and processes should be implemented not only because they appear in standards and best practices, but also because they are relevant in the current situation. (Diesch et al., 2020) Therefore, Based on the evidences presented above:-

H_1: Considering the Existing organization Infrastructure has significant effect on information system security investment.

ix. Considering Future growth

According to (Eric, 2018) outlines, before selecting a security solution, consider long and short term growth goals and how they may impact security demand. Organizational business alignment and future growth should be considered through collaborative efforts between information security and business management in aligning ISMS practices with organizational business strategy (Maarop *et al.*, 2015). Have a Continuous IT and a disaster recovery strategy which are crucial, and they should periodically be tested (Diesch *et al.*, 2020). According to (Björck et al. 2015), continuity is the capacity to consistently deliver the desired result in the face of unfavourable cyber events. A "predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained before returning to normal operations" (NIST, 2017). With relates to (Kirubel, 2022) Confirmed Not considering future growth is one of the factor influencing information system security investment. Therefore, Based on the evidences presented above:-

H_1: Considering future growth has significant effect on information system security investment.

x. Legal and regulatory frameworks

legal and regulatory frameworks are rules, standards and regulations that include a list of controls and policy which guide and support information system security (Schatz and Bashroush, 2018).Several laws implemented with the primary agenda of protecting data in organizations and securing computer systems (Lee, 2021). Most organizations adopt/create IS security policies in order to comply with international standards or governments; Regulations and rules frequently have an impact on information security investments by providing

guidance on a minimal begin investment baseline, a list of controls to consider, and support in detecting gaps and vulnerabilities (Schatz and Bashroush, 2018). Policies guarantee that technology resources are managed properly (Watters & Ziegler, 2016).

The most frequently stated force influencing firms' investment plan was regulations (Rowe *et al.*, 2006). Country factors, such as legislative frameworks, rules, and acts that place great pressure on enterprises, are the primary external drivers for decisions to invest in information security. The same is true for industry-specific rules and trading partner criteria (Weishäupl et al., 2018). According to (Lopes and Oliveira, 2015), policy implementation issues exist because most rules are established for compliance purposes rather than actual security concerns. The organization could discover implementation and investment obstacles, constraints, and technology advances that require policy considerations with proper execution of Information Security policies (Alotaib, & Clarke, 2016).As stated by (Kirubel, 2022), it is critical to consider frameworks and standards when making a decision since they serve as a roadmap for managing the risks that are connected with living in a digital environment. Beside, organizations can minimize security breaches by tightening law and regulations and investing in security products or services (lee *et al.*, 2018). According to (Parsons *et al.*, 2015). In the context of information security, offering incentives may encourage inventive strategies to conceal breaches rather than improvements in information security decision making. To maximize the effectiveness of its activities, the lawmaker/principal/steward must consider the impact of its actions on the formation of the norms that will now be anticipated to prevail while establishing the regulatory framework and other obligations/incentives (Ioannidis *et al.*, 2016). It will be important to reinforce the law, monitor and penalize punishment responsible person in case of security breach (lee *et al* 2018), and top management will also monitor the ISM implementation to guarantee it is constantly on track (Hashim and Razil, 2019). According to (Temtim and Alpha, 2019) states, the audit and monitoring processes increase information system security compliance in organizations by delivering immediate data regarding to undesirable employee behaviour. Therefore, Based on the evidences presented above:-

H_1: Legal and regulatory frameworks has significant effect on information system security investment.

xi. Vendor Involvement

Vendor involvement is the involvement of vendors the relationship with the service providers, third party partners and suppliers of information security solutions. According to (Chatzoglou *et al.,* 2017) stated, Vendor involvement has an advantage since vendor provide support on technology, training, assistance during adoption, or system updates through vendors or consultants. According to (Kirubel, 2022) Vendors, have been known to interfere in an organization's internal affairs in order to select security solutions. Therefore, Based on the evidences presented above:-

H_1: Vendor involvement has significant effect on information system security investment.

xii. Experience on security incidents

Experience of security incidents is defined as the likelihood, previous history and severity of security breaches **(**Lee *et al.,* 2018**)**. Security incidents, in particular, appear to be a significant motivator for security investment (Schatz and Bashroush, 2018). Budgeting for cyber resilience can be difficult because no recent cyber incidents have occurred to evaluate costs and effects. Furthermore, budgeting changes between an organization that predicts solely opportunistic attacks and a business that may be targeted for an attack since budget allocation may vary based on the kinds of attacks that the firm anticipates (Carías *et al.,* 2019). The absence of a cyber event in the organization should be used to assess the risk that each information set will be subjected to a cyber security breach, which has a substantial impact on security investment (Gordon *et al.,* 2015).Security incidents has a direct impact on information security investments. Internal information security concerns of the organization are virtually overlooked, especially when considering "accidental" occurrences. Most organizations do not consider internal incidents such as unintended file deletion or password sharing to be serious security incidents, particularly an inability to secure a sensitive document (Ng *et al.,* 2013). Understanding threat trends is vital for leading security initiatives and allocating money appropriately. Organizations went through security breaches prior are more likely to enhance their information security investment to mitigate risk, depending on the extent and rate of the occurrences (Lee *et al.,* 2018). Therefore, Based on the evidences presented above:-

H_1: Experience on Security incidents has significant effect on information system security investment.

xiii. Decision support processes

Decision support process is a process which uses decision making resources and scientific methodologies to make more evidence based decisions on information system security (Zhao et al., 2013). The absence of tools that supports decisions and evidence-based information has a significant influence for information system security investment (Schatz and Bashroush, 2018). Each stakeholder is willing to help whoever it is which is significant to him or her. In certain circumstances, decision making experienced difficulties by a lack of shared language (Toivannen, 2015).

Managers may find it difficult to build effective cyber resilience measures, particularly when assessing how much money would need to be invested in such approaches before the organization encounters cyber disasters (Carias *et al.,* 2019). Organizations invest in technical security resources without any standardized decision processes, and the decision process is biased and dependent on organizational and psychological factors (Weishäupl *et al.,* 2018).

Normal investors have constraints in processing a massive amount of financial information; therefore they depend on heuristics (a problem-solving strategy that uses shortcuts to provide good-enough solutions given a limited time frame or deadline). This could result in prejudice or less-than-optimal decisions (Aigbovo and Ilaboya, 2019). The decision to invest in technical and human factors is usually based on the gut feelings or informal discussion with managers, CISO without proper model (Parsons *et al.,* 2022). Senior management and supervisors should talk about information security initiatives more frequently (Shao *et al.,* 2019). Therefore, Based on the evidences presented above:-

H_1: Decision support process has significant effect on information system security investment.

xiv. Financial Evaluation models

It is an approach and evaluation method which used for determining the optimal level of investment (Ekelund and iskoujina, 2019). Financial assessments assist in identifying the assets, dangers, and vulnerabilities of information systems and provide a strategy for the required investment. According to (Weishäupl et al 2017) Analyzing Information security

investment is a challenging process because the return of investment whether it is tangible or intangible is impossible to estimate based on this the organization is uncertain to invest. Knowing the appropriate investment level, the organization takes into account all important elements and decides how to allocate the money among the countermeasures identified for possible investment (Zhuo, 2019).

According to (Moore *et al.,* 2010), estimating return on investment (ROI) is possible and even beneficial in some circumstances, but it is not always the right metric to use. Evaluation techniques, like decision processes, are rarely utilized in practice to assess the effectiveness and efficiency of information security investments (Weishäupl *et al.,* 2018). There are different financial evaluation approaches. A valuation method known as net present value determines the present worth of an investment's future cash flows (Bojanc *et al.,* 2008).In addition, A return on investment formula measures an investment's effectiveness based on its cost and anticipated return (Bryan & Zuva, 2021. Even if the return on security investment is easily calculated, human decision-makers struggle to determine the optimal security investment value (Safi 2016). Financial evaluation or performance models are used once in blue moon (Schatz and Bashroush, 2018). Due to this, Decision makers are unsure about the intangible costs and benefits of information security investments. Therefore, Based on the evidences presented above:-

H_1: Financial Evaluation models have significant effect on information system security investment.

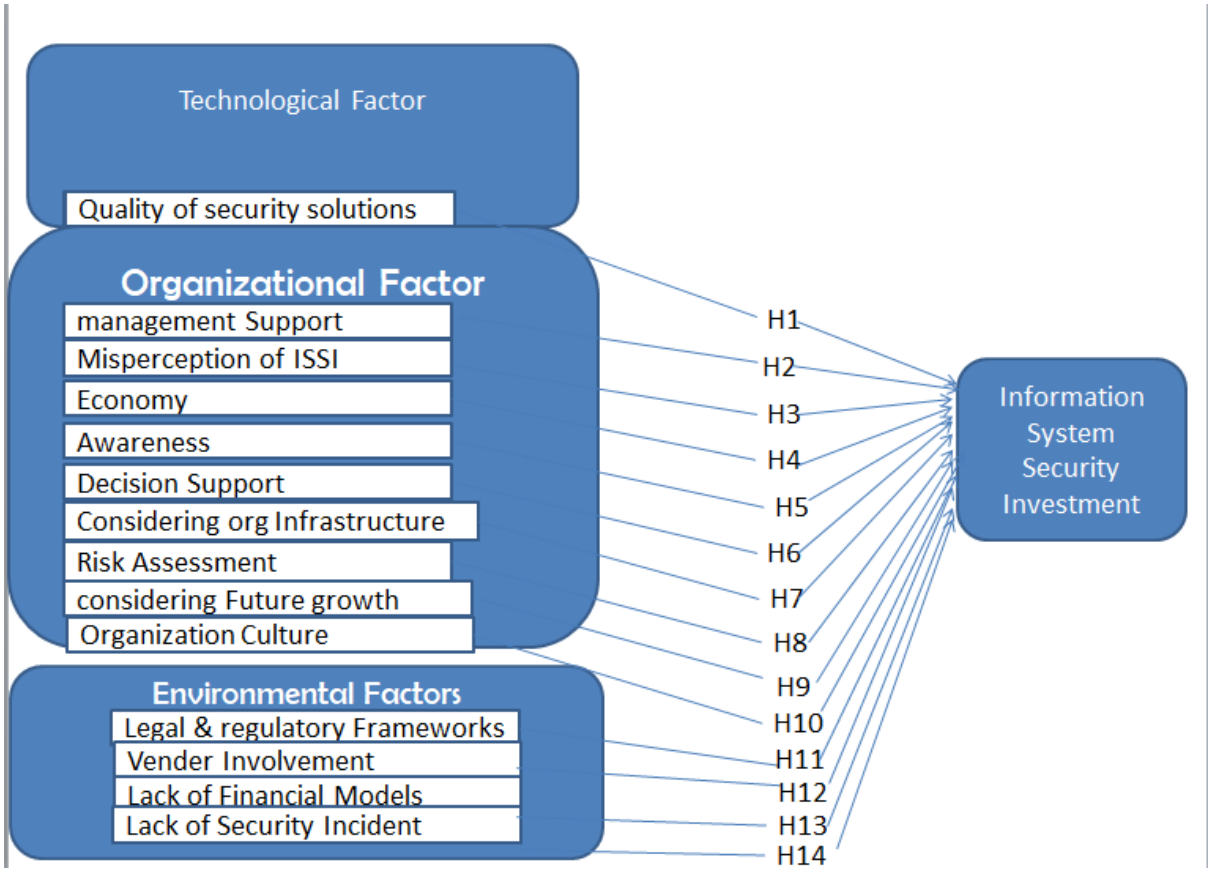

Figure 2-1: Conceptual framework of the study

2.14. Chapter Summary

In this section, works of literature that are related to information system security and investment are reviewed. The chapter consists of the following major topics: introduction to information system, information systems security, information security management, major information systems assets, Major threats and vulnerabilities in information security assets, information system security controls, Information systems security in public organizations, Information system security risk management in public organizations, information technology investment, Information systems security investment, The Technology, organization and Environment framework, factors affecting Information systems security investment in public organizations, review of related works have been reviewed. A conceptual framework is also developed based on the factors identified from extant literature. Next chapter, chapter three, deals with the research design and methods.

CHAPTER 3: RESEARCH METHODOLOGY

This chapter explores the research methodology that was used in carrying out the research. The research approach, Research Design, Population of the study, Sampling Technique, data collection technique, Analytical tool, Validity and Reliability of the study is explained in this chapter.

3.1. Research Approach, and Research Design

3.1.1. Research Approach/ Method

The Study used a Quantitative research methodology which was suitable for addressing to the research questions. The quantitative research approach employs inquiry methods which include experiments and surveys to collect data on predefined instruments that yield statistical data (Creswell *et al.,* 2014).

3.1.2. Research Design

Research Design is sequential action plan for investigating and answering research questions. It contributes to ensuring that research issues are adequately addressed (Kothari, 2004). The study employs both descriptive and explanatory research design. Descriptive analysis assists in describing or summarizing the characteristics of a dataset in a constructive manner. The explanatory approach was applied since it tries to explain the link between the dependent and independent variables, which are information system security investments and factors influencing information system security investment.

3.2. Description of Target Population, and sample size

3.2.1. Expert Selection

According to (Bogner *et al.,* 2014), an expert is a person who has specialized practical or experimental knowledge about a certain problem area or field of study and is able to organize that knowledge in a way that is relevant and action-guiding for others. This definition served as the basis for choosing the target populations. As a result, an expert should have a significant amount of experience in the subject of information security, which indicates that they have specialized practical knowledge in that area. The expert should hold a position of authority or decision making inside the company, demonstrating their aptitude for organizing knowledge in a way that is both useful and conducive to action. According to (Karjalainen *et al.,* 2014) information system security investment decision are mainly driven by information

specialists and organization decision makers. Additionally, a leading position promotes the fundamental, all-encompassing perspective that is necessary for the research's objective. The populations of the study are organization decision makers and personnel's who has direct attachment with information system security Investment includes, Chief information officer, Chief security officer, Senior ICT Experts, Team leaders, Managers and Directors. This study applied census inquiry complete enumeration of populations due to small number of population. According to (Vaus & Vaus, 2013), A census method is a statistical investigation in which the data are collected for each and every element or unit of the population.

3.2.2. Selection of Public Organizations

The study was conducted in Eight Ethiopian public organizations. For selecting public organizations, the researcher employed the convenience sampling method. Since, information security information is kept private, as a result of this limitation; many organizations refuse to share data about themselves. Due to this, the researcher chooses convenient organizations for data collecting, allowing the researcher to obtain data that is easily accessible.

The selected organizations are, Ethiopian Public Health Institute, Information network security Agency, Federal Supreme court, Ministry of Education, Ministry of Health, Ministry of innovation and technology and Ministry of Revenue and Ministry of transport.

3.2.3. Description of Study Area

Ministry of Education is a government department of Ethiopia, focusing in the governance and policies of education. It is responsible for overseeing the teaching and learning process throughout the country from elementary school education to higher secondary school education. It regulates the general curriculum of public schools and also sets the precedent for private schools. In addition the ministry is the responsible for the Ethiopian National Exams. The Ministry has begun projects to improve and introduce technology as a means to alleviate chronic problems faced in the educational sector.(*Ministry of Education Ethiopia*, n.d.)

Federal Supreme court; - is governmental institution of, besides providing the organization mission, the court is establishing and investing different system. Currently, Ethiopian federal supreme court is deploying judicial system collaborates with Ethio-telecom. The implementation of ICT in Ethiopian Federal Court is a significant step towards modernizing the justice system (Ethiopian supreme court, 2023).

Ministry of Health; - is a governmental body which has an objective of promoting health and wellbeing of the society. One of the strategies of ministry of health is the deployment of

ICT in Ethiopia's health-care system. The key benefit of implementing technology is that it can help the Health Minister's office improve the quality of health care services by delivering accurate and timely health data. Healthcare providers in Ethiopia can use technology to monitor and track numerous healthcare issues such as disease outbreaks, patient information, and medical supplies. Ministry of Health deploys more than 17 systems so far that assist the Health Minister in making more informed decisions, allocating resources more effectively, and ultimately improving patient outcomes (Ministry of health-Ethiopia, n.d)

Minister of transport

The Ethiopian Ministry of Transport's adoption of information and communication technology (ICT) has substantially increased its production and efficiency. ICT has changed the way the Ministry does business, from service delivery to policy formation and implementation. One of the primary areas where ICT has been used in the Ministry of Transport is the development of computerized systems that streamline the Ministry's different activities.

Minister of revenue

The Ethiopian Ministry of revenue is governmental organization working on collecting taxes. One of the strategies of the organization is deployment of Information and Communication Technology (ICT) has had a considerable impact on how tax collection is carried out in the country. The overall efficiency and effectiveness of tax collection have been improved by integrating technology throughout the ministry. The Ministry uses the different computerized systems to facilitate tax collection, filing, and payment is one of the primary areas where ICT has been used in the Ministry.

Ethiopian public health institute

The use of ICT in EPHI has the potential to improve its operations and health results for the Ethiopian people. Digital laboratory health solutions are deployed in the organization... Electronic health records (EHRs), Gx Expert, Medx and other mobile health system are deployed in the organization.

Information network Agency

INSA's deployment of ICT can help strengthen its ability to protect Ethiopia's information network. Cyber security solutions are one important area where ICT can be used. With an increasing number of cyber threats, deploying sophisticated cyber security measures can assist INSA in protecting the country's information network from various cyber security dangers such as hacking, viruses, and malware. It entails, among other things, the installation of firewalls, antivirus software, and intrusion detection systems. Another area where ICT can

be used to benefit INSA is data management and analysis. With the increasing amount of data available to INSA, advanced data analysis techniques and systems can assist the agency in identifying patterns and trends (INSA, n.d)

Ministry of Technology and innovation

Ethiopia's Ministry of Technology and Innovation (MTI) is in charge of developing and regulating the country's technology and innovation sector's development. The use of ICT in the ministry can help them fulfill their objectives more efficiently, effectively, and safely. One important area in which ICT can be used is in the development of e-government services. Implementing ICT solutions can improve the delivery of services to citizens and businesses, such as online application and payment processing. Effective e-government systems promote user trust by increasing transparency and accountability in government services. Another manner in which ICT might be used by the ministry is in the creation of digital infrastructures such as broadband networks and data centers. The creation of such infrastructure has the potential to improve internet access.

3.3. Method of Data Collection

Secondary data was used for supporting the study and to get the findings of other researchers in the area of the study. Relevant Information was also gathered from different secondary sources such as book, newspapers and different communication materials. The primary Data was gathered via questionnaire from employees and Directors of the selected organization.

The researcher used Google forms to distribute the questionnaire; this was helpful to ensure all questions are completed where one can not submit without completing all questions. Also, to ensure all questions are filled in correctly (e.g. no rating scale items have more than one entry per item, and no missed items) the researcher set different rules in the Google form such as response validation was set to exactly one which ensures only one check box can be checked for a question at a time. It means that the questionnaires are completed rapidly and on one occasion, i.e. it can gather data from many respondents simultaneously.

3.4. Data Collection Procedure

To conduct the quantitative data collection, the piloted questionnaire was made ready by including informative cover page about the purpose of the study and the rights of the

participants to be involved. Pilot test of the questionnaire was made at Addis Ababa university ICT directorate, by presenting an official letter written from school of information science, Addis Ababa University in support of the researcher. Then, after the instrument was adjusted based on the results of the pilot study, the actual data collection was also held in each sampled organization by presenting a support letter and getting permissions.

3.5. Analytical Tool

To better comprehend the connections between the elements that encourage the adoption of technology, numerous conceptual models and theoretical frameworks have been established. Several theories, such as the protection motivation theory, the unified theory of acceptance and use of technology (UTAUT), the technology acceptance model (TAM) (Davis 1989) have been utilized to explain the process of technology adoption. The PMT, TAM and UTAUT theories are widely used to explain the adoption of technology since they focus on elements like individual attitudes and customer perceptions. However, TOE is more frequently used to analyze the technology adoption process since it looks at aspects linked to technology, the organization, and the environment (Cao et al., 2018). The TOE model, which provides a helpful analytical framework for examining the assimilation of various types of innovation at the organizational level and takes into account technological, organizational and Environmental factors has been used and modified in a number of technology adoption studies (Oliveira and Martins, 2011).

	Models	Description	Criticism
1	TECHNOLOGY ACCEPTANCE MODEL (TAM)	➢ Developed by Fred Davis in 1989 Modification of the Theory of Reasoned Action (Ajzen, 1991). ➢ Determines individual desires on adoption and use of new technologies in a professional setting (Bryan and Zuva, 2021) ➢ The Intention to use new technology is based factors: perceived usefulness and perceived ease of use. (Davis,1989)	➢ TAM: Originally developed for the adoption of IT at the workplace. The key feature of this model is its emphasis on the perceptions of the potential user. (Au and Zafar, 2008). ➢ TAM disregards the variety of needs pertinent to voluntary consumers. One of the main criticisms of the original TAM is particularly the absence of subjective norms or social impact (Autry *et al.*, 2010)
2	Protection Motivation Theory	➢ The PMT (Protection Motivation Theory) was put forth by Rogers in 1975 as a way to predict how someone could react to a call to fear. According to the theory that cognitive processes (such as threat and coping evaluation) lead to behavioural changes. (lee *et al.*, 2021) ➢ In the field of information security, the fear appeal or PMT has been used to explain some information security behaviours (lee *et al.*, 2021)	➢ It is related only to the behavioural intent to adopt security countermeasures to risks since the PMT is concerned with reducing or preventing dangers. it elucidates particular information security behaviours (Hasani *et al.*, 2023)

3	Unified Theory of Acceptance and Use of Technology	➢ The UTAUT, which stands for Unified Theory of Acceptance and Use of Technology, aims to offer a comprehensive understanding of all aspects that affect a person's behaviour while considering using a new technology. (Venkatesh *et al., 2003*)	➢ Unified Theory of Acceptance and utilize of Technology exclusively concentrates on user behaviour and behavioural intention to utilize a new technology.

A Technology organization Environment (T-O-E) Model was used in the study. Its advantage over other behavior models is that it reflects how different factors (both internal and external) affect adoption decisions. It is not limited on focusing behavioral intention like PMT, TAM and UTAUT. The TOE framework examines how decisions about adopting are made. The paradigm contends that elements influencing adoption decision-making include organizational traits, environmental conditions, and current technology (Wallace *et al.*, 2021). The TOE framework discusses and examines the implications of organizational, environmental, and technical elements on the adoption of technology from an organization perspective (Kim and Kim, 2021). According to (Alhogail *et al.*, 2015) technology states that adoption is influenced by the Range of technologies available to the company, as well as their perceived value, organizational and technological compatibility, complexity, etc. Organizational measures include the business scope of the company, top management support, organizational culture, the complexity of the managerial structure as measured by centralization, formalization, and vertical differentiation, the caliber of the human resources, and size-related issues like internal slack resources and specialization (Sabherwal *et al.*, 2006). Environment is related to those operational facilitators and inhibitors; major factors among them include competitive pressure, the preparedness of trading partners, sociocultural challenges, government encouragement, and technology support infrastructures like access to quality ICT consultants (Dor and Elovci, 2016).With respect to this the researcher use this TOE framework in the study to find out the effects of technical, organizational, and

environmental factors regarding information security investment decisions. The TOE framework is relevant for cyber security adoption decisions (Wallace *et al.*, 2021).

3.6. Method of Data Analysis

The data collected through questionnaires was coded and entered into a computer for further analysis. The data was analyzed using the Statistical Package for Social Science (SPSS – version 23) which can run basic descriptive and inferential statistics used. Descriptive statistics like measures of frequency, percentages, means, standard deviations and inferential statistics such as multiple regressions were used to analyze the quantitative data. The presentation, discussion and interpretation of results were made. Background information of respondents was interpreted and analyzed using descriptive statistics. Specifically, the demographic characteristics of the respondents were presented based on sex, academic rank, occupation status. Then correlation and multiple regressions were used for analysis of the quantitative data mainly based on the nature of the research questions.

To analyze the relationship between dependent (information system security investment) and independent variables (those factors affecting information system investment), Pearson-moment correlation coefficient was used. The values for correlation (r) which indicate the statistical relationship between the dependent and independent variables. This means, the value of +1 indicates a perfect positive correlation and a value of -1 indicates perfect negative correlation dependent and independent variables. Therefore, the closer the value (r) to positive 1, strong positive relationship exists between the dependent and independent variables and vice versa.

A detailed interpretation of the coefficient of correlation by researchers was also done for this study. In addition, coefficient of determination (r^2) was also calculated to find out the amount of variation in the dependent variables which explains its relationship with the independent variables. Finally, multiple linear regression analysis was carried out to investigate the difference between effect of two or more independent variables and the individual effect on the dependent variables.

3.7. Validity and reliability

3.7.1. Validity

Validity and Reliability is used for examining the quality of research. According to (Heale & Twycross, 2015) Validity is the level of accuracy which a notion is measured in an investigation of a study.

According to (Kothari, 2004) the questionnaire's internal validity refers to its ability to measure what it intended to measure. In other words what is found with the questionnaire actually represents the reality of what is measured. For this purpose, the questionnaire was piloted before the actual dissemination for data collection, to check its validity and reliability; In light of this the researcher used pilot study and expert validity technique to validate quantitative data.

3.7.2. Reliability

The extent to which scientific study yields solid and consistent outcomes is measured by its reliability (Carmines and Zeller 1979). According to (Cavana *et al.*, 2001) Reliability is the extent to which a measurement is error-free and, as a result, produces consistent findings. The researcher applied cronbach's alpha coefficient to measure internal consistency. According to (Gliem & Gliem 2003) states Cronbach's alpha reliability coefficient normally ranges between 0 and 1. The closer Cronbach's alpha coefficient to 1.0 the greater the internal consistency of the items in the scale. According to (Kothari 2004) the cronbach's alpha result of 0.7 and above implies an acceptable level of internal reliability.

The study's constructs' internal consistency is gauged by their reliability. If a construct's Alpha Value is higher than 0.70, it is considered reliable. Table 3-1 presents the Cronbach alpha of each variable.

Table 3.1: Reliability Test

Variable	Cronbach Alpha	Items
Management Support	.897	4
Misperception of ISS	.665	4
Economy	.802	3
Legal and regulatory framework	.908	4
Experience on security incident	.710	3

Awareness	.855	3
Decision support process	.823	4
Finical evaluation Model	.908	3
Organization Culture	.869	4
Risk Assessment	.924	3
Consideration of organization structure	.830	3
Future growth	.883	3
Vendor management	.733	3
Quality of ISS	.834	3

Source: SPSS Version 23, Output

3.8. Ethical Consideration

The researcher made use of different data collection instruments from different sources. Utmost effort it's exerted to acknowledge materials referred & the researcher takes the responsibility to keep confidentiality of respondents' opinions & unanimity of the rest of the information. The researcher thus will ensure that all participants are treated with respect and dignity, after being informed that the study is voluntary and no discrimination will be triggered by failure to participate. Identification codes will be assigned to the filled questionnaires, rather than participant names, to ensure that the participants received absolute confidentiality. The data gathered from respondents will be used exclusively for the purposes of the study and will not be given to third parties for any other purpose. Accordingly, the researcher optimally considers all the ethical perspectives.

3.9. Chapter Summary

This chapter explored the research methodology and design that was used in carrying out the research study by describing the research approach, research design, population and sampling, sources of data and types, data collection procedure and finally data analysis. Next chapter deals with result and discussions of the study.

CHAPTER 4: DATA PRESENTATION, ANALYSIS, AND INTERPRETATION

The study's findings, including hypotheses testing, are presented and discussed in the following paragraphs.

4.1. Data Presentation

4.1.1. Response Rate

The frequency of the data collected from each organization is presented in table 4.1.

Table 4.1: Frequency of the data collected from each organization

Organization	Frequency	Percent	Valid Percent	Cumulative Percent
Ethiopian Public Health Institute	10	11.6	11.6	11.6
Federal Supreme Court	9	10.5	10.5	22.1
Information Network Security Agency	13	15.1	15.1	37.2
Ministry of Education	9	10.5	10.5	47.7
Ministry of Health	13	15.1	15.1	62.8
Ministry of Innovation and Technology	7	8.1	8.1	70.9
Ministry of Revenue	19	22.1	22.1	93.0
Ministry of Transport	6	7.0	7.0	100.0
Total	**86**	**100.0**	**100.0**	

Source: SPSS Version 23, Output

Table 4.2 shows the total number questioners distributed and collected from eight organizations. Questionnaires are distributed across Ethiopian Public Health Institute, Federal Supreme Court, Information Network Security Agency, Ministry of Education, Ministry of Health, Ministry of innovation and technology, Ministry of Revenue and Ministry of Transport. The number of questionnaires distributed depends on the number of personnel's who has direct attachment with Information system security investment. In general, the total number of questionnaires distributed was 105 and the returned questionnaires are 86 with a response rate of 81.9 %.

Table 4.2: Number of distributed and collected questionnaire

	Name Of Organization	Number of Questioners		
		Distributed	Collected	Percentage (%)
2	Ethiopian Public Health Institute	10	10	100%
3	Federal Supreme Court	10	9	90%
4	Information Network Security Agency	20	13	65%
5	Ministry Of Education	10	9	90%
6	Ministry of Health	15	13	86.6%
7	Ministry of Innovation and Technology	10	7	70%
8	Ministry of Revenue	20	19	95%
9	Ministry of Transport	10	6	60%
	Total	**105**	**86**	**81.9%**

Source: SPSS Version 23, Output

Table 4.2 shows, the respondent rate of organizations. From Ethiopian public health institute, Out of the total 10 questionnaires distributed, 10 of the questionnaires are returned. From the total number of 10 questionnaires distributed to Federal Supreme Court, 9 of the questionnaires are collected. From the total number of 20 questionnaires distributed to Information Network Security Agency, 13 of the questionnaires are collected. From the total number of 10 questionnaires distributed to Ministry Of Education, 9 of the questionnaires are collected. From the total number of 15 questionnaires distributed to Ministry Of Health, 13 of the questionnaires are collected. From the total number of 10 questionnaires distributed to Ministry of Innovation and Technology, 7 of the questionnaires are collected. From the total number of 20 questionnaires distributed to Ministry of Revenue, 19 of the questionnaires are collected. From the total number of 10 questionnaires distributed to Ministry of Transport, 6 of the questionnaires are collected. In general, the total number of questionnaires distributed to eight organizations was 105 and the returned questionnaires are 86 with a response rate of 81.9%.

4.1.2. Demographic Characteristics of Respondents

This portion of the survey is concerned with background of the respondents to understand the employees or respondents who participate in filling the questionnaire for this research.

Respondents are requested to fill their sex, their level of education and their present occupation status in the organization.

Table 4.3: Demographic Data of Respondents

Variable	Category	Frequency	Percentage (%)
Gender	Male	56	65.1
	Female	30	34.9
	Total	**86**	**100.0**
Level of Education	Certificate	2	2.3
	College Diploma	3	3.5
	Undergraduate	29	33.7
	Masters	50	58.1
	Ph.D.	1	1.2
	Missing	1	1.2
	Total	86	100.0
Occupation	Chief Information Officer(CIO)	8.0	9.3
	Chief Security Officer(CSO)	9.0	10.5
	Department Head	17	19.8
	Director	6	7.0
	ICT Senior Expert	41	47.7
	Others	5	5.8
	Total	86	100.0

Source: SPSS Version 23 Output, 2023

Table 4.3 presents the demographic data of respondents. The study shows that 65.1 % of the respondents are males whereas only 34.9 % of the respondents are females. This is not good representation of sex and shows there is no sex equity. Hence due to the research questions being free of any gender view, it can be concluded that both of their views were considered in the study.

As it is depicted in, table 4.3 the distribution of respondents by the level of education showed that, the majority of the respondents is Master degree holders with the percentage of 58.1%. Whereas 33.7% of the respondents have first degree. 3.5% of the respondents have College diploma and only 2.3% are certificate level employees. 1.2% of respondent have Ph.D. This made the researcher to believe that the respondents were educated to the level to understand the issues factor affected information system security investment. Respondents with technical knowledge of the research topic are useful in the research process because they help gather accurate and trustworthy data on the topic at hand.

From the findings, With regards to occupation status, the majority of Respondents are ICT Senior Experts with the percentage of 47.7%. Whereas 19.8 % of them are Department Heads. 10.5 % of them are Chief Security Officers. 7.0 % of them are Directors. 9.3% of them are Chief Information Officers. Others account 5.8%. This shows that the survey respondents are personnel's who have direct attachment with information system security investment decisions. These findings made the researcher believe that the respondents were at a level to understand the issues related to the study objectives.

4.2. Descriptive Statistical Analysis

The respondents were asked to indicate their level of agreement to the statements explaining the factors affecting information system security investment. The variables are organized under the TOE factors, the results are organized in percentage for each factor with respect to the level of agreement (strongly agree, agree, neutral, disagree, and strongly disagree) as shown in Table 4.3 below.

4.2.1. Technology Context

4.2.1.1. Quality of information system security solutions

As depicts on Table 4.17, the majority of respondents disagree response on the statement, the existing information system security solutions are not complex and easy to use. The majority of respondents provide disagree response on the statement. Majority of respondent are neutral on the information system security solutions are flexible and the Majority of respondents disagree with organization information system security solutions has a reliable functionality.

Table 4.4: Descriptive Statistics for the items used to measure Quality of information system security solutions

Items	Mean	Std. Deviation
The existing information system security solutions are not complex and easy to use.	2.92	.871
The information system security solutions are flexible	3.08	1.108
Your organization information system security solutions has a reliable functionality	2.72	1.155

Source: SPSS Version 23 Output, 2023

4.2.2. Organizational Context

4.2.2.1. Management support

As the table 4.4 Indicates, The majority of respondents are neutral in the statement of organization's management does demonstrates a commitment to enforcing information security polices across the organization. Regarding to the management does budget for facilities such as organizing security awareness workshops, majority of respondents are neutral. With respect to the management does budget for resources for the implementation of

the Information system security in the organization, Majority of the respondents disagrees. Regarding to the management does prioritize information security just like other core business issues. Majority of respondents are disagrees with the statement.

Table 4.5: Descriptive Statistics for the items used to measure lack of Management support

Items	Mean	Std. Deviation
Your organization's management demonstrates a commitment to enforcing information security polices across the organization.	3.26	1.257
The management does budget for facilities such as organizing security awareness workshops.	3.12	1.121
The management does budget for resources for the implementation of the Information system security in the organization.	2.98	1.265
The management does prioritize information security just like other core business issues.	2.93	1.186

Source: SPSS Version 23 Output, 2023

4.2.2.2. Misperception of information system security

As the table 4.5 Indicates, The majority of respondents are neutral in the statement of organization pay attention to external threats like viruses while consistently underestimating the severity of internal problems. Regarding to Organization does perceive that they are powerless to stop a concerted, premeditated attack. The majority of respondent has a neutral response with the statement. With respect to the statement Organization does believe that investing in information systems security reduces an organization's productivity, profitability and business operations, majority of the respondent has a neutral response. The majority of respondents are neutral in the statement of organization does perceive the type of business they are in isn't going to be attacked.

Table 4.6: Descriptive Statistics for the items used to measure Misperception of information system security

Items	Mean	Std. Deviation
Your organization pay attention to external threats like viruses while consistently underestimating the severity of internal problems	3.60	.924
Organization does perceive that they are powerless to stop a concerted, premeditated attack.	3.08	1.054
Your Organization does believe that spending in information systems security reduces an organization's productivity, profitability and business operations.	3.31	1.230
Your organization does perceive the type of business they are in isn't going to be attacked.	3.27	1.222

Source: SPSS Version 23 Output, 2023

4.2.2.3. Economy

As the table 4.6 Indicates, The majority of respondents are neutral with the statement of organization does fund sufficient budget to spend in information systems security solutions. Regarding to organization is required to boost its budget if the organization damages are maximum or existent the majority of respondents are neutral meanwhile, with the statement of organization does provide budget to hiring security specialists the majority of respondents neutral.

Table 4.7: Descriptive Statistics for the items used to measure Economy

Items	Mean	Std. Deviation
Your organization does fund sufficient budget to spend in information systems security solutions	3.14	1.219
Your organization is required to boost its budget if the organization damages are maximum or existent	3.09	1.059
Your organization does funds to hire security specialists	3.20	1.050

Source: SPSS Version 23 Output, 2023

4.2.2.4. Awareness

As the tables 4.9 Indicates, The majority of respondents are neutral with the statement of the management is technologically educated, and does have a background on ICT or cyber

security. The majority of respondents disagree with the statement of There is no dearth of knowledge and experience in information security among security personnel's. The majority of respondents disagree with the statement of decision on the security are made with occurrence of incident, probability of outcomes or effects.

Table 4.8: Descriptive Statistics for the items used to measure Awareness

Items	Mean	Std. Deviation
Your organization management is technologically educated, and does have a background on ICT	3.03	1.241
There is no dearth of knowledge and experience in information security among security personnel's	2.65	1.026
Information system security decisions are made with considering the likelihood of occurrence, the probabilities of the outcomes, or the consequences.	2.74	.923

Source: SPSS Version 23 Output, 2023

4.2.2.5. Decision support process

As depicts on Table 4.10 the majority of respondents disagree with the statements of there is Evidence based decision making procedures. On statement the decision to invest in information security relies on agreement between CISO and CIO with using proper multi-stakeholder decision models or approaches, the majority of respondents disagrees. Meanwhile, the majority of respondents provide disagree response on the statement of There is a common language due to that each stakeholders in the organization is eager to assist the one essential to himself/herself. The majority of respondents disagrees response with the statements of there is no Organizational and psychological bias on organizational decision making

Table 4.9: Descriptive Statistics for the items used to measure Decision support process

Items	Mean	Std. Deviation
There is Evidence based decision making procedures	2.83	1.020
The decision is based on agreement between managers and CSIO with standardized model	2.64	.957

There is a common language due to that each stakeholders in the organization is eager to assist the one essential to himself/herself	2.62	1.042
There is no organizational and psychological bias on organizational decision making	2.63	1.052

Source: SPSS Version 23 Output, 2023

4.2.2.6. Considering of the existing Organization Infrastructure

As depicts on Table 4.14 the majority of the respondent disagree with the statement your organization utilize prior experience from other organizations and compare and contrast with its existing security solution. With Relates to Your organization verify whether security solutions are compatible with the organization's infrastructure before investing, majority of the respondent disagree. Regarding to the statement your organization does convey various stakeholders in an effective manner for investing information security solutions majority of the respondent provides disagree response.

Table 4.10: Descriptive Statistics for the items used to measure Not Considering of the existing Organization Infrastructure

Items	Mean	Std. Deviation
Your organization utilize prior experience from other organizations and compare and contrast with its existing security solution	2.86	.932
Your organization verifies whether security solutions are compatible with the organization's infrastructure before investing.	2.78	.938
Your organization does convey various stakeholders in an effective manner for investing information security solutions.	2.81	.888

Source: SPSS Version 23 Output, 2023

4.2.2.7. Risk Assessment

As depicts on Table 4.13 the majority of the respondent provides neutral response on organization determines and classifies valuable assets and focus on how to protect them. With respect to your organization has an approach for recognizing and evaluating operational risks, the majority of respondent provides neutral response. With relates to a statement your

organization acknowledge of what it should be secure to and control strategies, the majority of respondent provides neutral response.

Table 4.11: Descriptive Statistics for the items used to measure Risk assessment

Items	Mean	Std. Deviation
Your organization determines and classifies valuable assets and focus on how to protect them	3.08	1.190
Your organization has an approach for recognizing and evaluating operational risks.	3.21	.959
Your organization has acknowledge of what it should be secure to and control strategies	3.16	.956

Source: SPSS Version 23 Output, 2023

4.2.2.8. Considering future growth

As depicts on Table 4.15, the majority of respondents provide neutral response on Your Organization establish its long and short-term growth objectives before choosing a security solution. Regarding with the statement organization security investments are sync with the organization mission, the majority of respondents provide neutral response and with relates to the statement there is effective information system security investment strategy or implementation; the majority of respondents provide neutral response with the statement.

Table 4.12: Descriptive Statistics for the items used to measure Not Considering future growth

Items	Mean	Std. Deviation
Your Organization establishes its long and short-term growth objectives before choosing a security solution.	3.06	.912
Your organization security investments are sync with the organization mission.	3.14	1.170
There is effective information system security investment strategy or implementation.	3.01	1.035

Source: SPSS Version 23 Output, 2023

4.2.2.9. Organization information system security culture

As depicts on Table 4.12 the majority of respondents provide neutral response with the statements of based on the type of business the Organization has topic or mission for information security. Regarding to the statement there exists a consciousness of the necessity of information security due to this there is IS specialist and IS department in the organization, majority of the respondent disagrees. With respect to the statement there is cooperation between information security and business managers in aligning ISMS practices with organization mission, the majority of the respondent disagrees. Regard to the statement Organization does establish an information security focus or does emphasis norms among all employees; majority of the respondent disagrees with the statement.

Table 4.13: Descriptive Statistics for the items used to measure Organization culture

Items	Mean	Std. Deviation
Based on the type of business the Organization has topic or mission for information security	3.21	1.086
There exists a consciousness of the necessity of information security due to this there is IS specialist and IS department in the organization.	2.58	1.122
There is cooperation between security specialists and business managers in aligning ISMS practices with organization mission.	2.49	1.082
Organization establishes an information security focus or does not emphasis norms among all employees	2.60	1.021

Source: SPSS Version 23 Output, 2023

4.2.3. Environmental Context

4.2.3.1. Legal and regulatory framework

As the tables 4.7 Indicates, The majority of respondents are disagree with the statement of organization utilize international security standards. The majority of respondents are disagree with the statement of organization has established defined rules and criteria's for assessing and prioritizing information system security investment. With regard to Security policies are applied and provide ensures security majority of respondents are disagreeing. The majority of respondents are disagrees with the statement of organization conduct audit and monitoring, impose penalties in case of security investment practices.

Table 4.14: Descriptive Statistics for the items used to measure Economy

Items	Mean	Std. Deviation
Your organization utilizes international standard security frameworks.	2.97	1.023
Your Organization has established defined rules and criteria's for assessing and prioritizing information system security investment	2.78	1.056
Security policies are applied and provide ensures security.	2.85	1.057
Your organization conduct audit and monitoring, impose penalties in case of security investment practices.	2.65	1.049

Source: SPSS Version 23 Output, 2023

4.2.3.2. Vendor Involvement

As depicts on Table 4.16, the majority of respondents disagrees with there is extreme vendor involvement in selections of security solutions. The majority of respondents provide neutral response on the statement Vendor doesn't provides support and assistance in selection of information system security solutions. The majority of respondents provide neutral response on the statement there is no transparent communication and participation with vendors in selections of security solutions.

Table 4.15: Descriptive Statistics for the items used to measure Vendor management

Items	Mean	Std. Deviation
There is extreme vendor involvement in selections of security solutions.	2.98	.958
Vendor doesn't provide support and assistance in selections of security solutions.	3.01	.939
There is no transparent communication and participation with vendors in selections of security solutions.	3.15	1.163

Source: SPSS Version 23 Output, 2023

4.2.3.3. Financial Evaluation models

As depicts on Table 4.11 the majority of respondents provide disagree response with the statements of organization has ability to identify the monetary value of investment. With respect to the statement organization has a method for predicting how much money would

need to be invested before the organization experiencing cyber disaster, the majority of respondents disagrees. With regard to organization is convinced of expenditures and benefit of information security investments, the majority of respondents disagree.

Table 4.16: Descriptive Statistics for the items used to measure Financial Evaluation models

Items	Mean	Std. Deviation
Your organization has ability to identify the monetary value of investment.	2.72	.890
Your organization has a method for predicting how much money would need to be invested before the organization experiencing cyber disaster	2.53	1.037
Your organization is convinced of expenditures and benefit of information security investments	2.52	1.093

Source: SPSS Version 23 Output, 2023

4.2.3.4. Experience on Security incidents

As the tables 4.8 Indicates, The majority of respondents disagree with the statement of organization considers internal security incidents as a critical security incident. Majority of respondents disagree on the statement of Organization's budget for cyber protection is depending upon an incident of security event. The majority of respondents have provided disagree response on the statement of Decision makers are not biased towards spending on information security measures.

Table 4.17: Descriptive Statistics for the items used to measure Experience on Security incidents

Items	Mean	Std. Deviation
Your organization considers internal security incidents as a critical security incident.	2.42	1.068
Your Organization's budget for cyber protection is depending upon an incident of security event.	2.74	1.170
Decision makers are not biased towards spending on information security measures.	2.66	1.123

Source: SPSS Version 23 Output, 2023

4.3. Correlation analysis

Correlation is analysis method to determine the degree of relationship between two variables and the direction of the relationship. The study examined correlation analysis to explore the relationship between variables and information system security investment. Correlation analysis is based on a correlation coefficient, which ranges from -1 to 1. .The study conducted correlation analysis at 99% confidence interval and 1% confidence level 2- tailed to identify which factors are most strongly associated with Information system security investment. Hence, Pearson's correlation coefficient is used since the variables being analyzed are continuous and normally distributed.

The correlational analysis matrix as shown in table4.19 reveals, From the Technological Context, Quality of information system security solutions has positive relationship with information system security investment with a Pearson coefficient value of .355 and p-value of .001.

Based on the correlational analysis matrix as shown in table4.19 reveals, from the organizational Context, There is a positive relationship between management Support and investment in information system security, with a Pearson correlation coefficient value of .499 and p-value of .000. Misperception of information system security has a negative relationship with Information system security investment with a coefficient value of -.321 and p-value of .003. There is a positive relationship between Economy and Information system security investment, with a Pearson coefficient value of .659 and p-value of .000. According to the correlational analysis, there is a positive relationship between Awareness and information system security Investment with a Pearson correlation coefficient value of .662 and p-value of .000. With a correlation coefficient of .136 and p-value of .210, the analysis found that a decision support process has a positive relationship with information system security investment. From the findings, there is a positive relationship between considering existing considering organization infrastructure and information system security investment with a Pearson correlation coefficient value of .484 and p-value of .000. From the findings, risk assessment has a positive relationship with investment, with a Pearson correlation coefficient value of .649 and p-value of .000.

From the findings, there is a positive relationship between considering future growth and information system security investment with a Pearson correlation coefficient value of .453

and p-value of .000. From the findings organization culture has a positive relationship with investment with a Pearson correlation coefficient value of .189 and p-value of .082.

Based on the correlational analysis clearly reveals, From the Environmental Context, legal and Regulatory Frameworks has a positive relationship with Information system security investment with P-value of .658 and correlation coefficient of .000. With respect to vendor involvement there is a negative relation with information system security investment with a Pearson correlation coefficient value of -.417 and p-value of .000. From the findings, financial model has positive relationship with investment, investment with a Pearson correlation coefficient value of .199 and p-value of .067. With a correlation coefficient of .017 and p-value of .880, Experience with security incidents has a positive relationship with Information system security investment.

Table 4.18: Correlation Matrix

	MS	MP	E	L	Ex	A	D	F	BC	R	OS	FG	VM	Q	Inv
MS	1														
MP	-.214	1													
E	-.746**	.313**	1												
L	.734**	-.377**	-.741**	1											
Ex	.121	-.244*	-.080	-.010	1										
A	-.716**	.309**	.728**	-.694**	-.041	1									
D	.479**	-.521**	-.456**	-.478**	.348**	-.446**	1								
F	.394**	-.408**	-.437**	-.448**	.293**	-.345**	.654**	1							
BC	-.469**	.357**	-.504**	-.476**	.215	-.422**	.642**	.716**	1						
R	.690**	-.279**	.741**	.787**	-.035	-.677**	.397**	.435**	.577**	1					
OS	-.653**	.213*	.724**	-.589**	-.058	.623**	-.446**	-.403**	-.516**	-.662**	1				
FG	.682**	-.238*	-.753**	.690**	-.069	-.723**	.539**	-.497**	.627**	.777**	-.817**	1			
VM	-.451**	.072	.439**	-.443**	.213*	.495**	-.250*	-.167	-.212	-.431**	.500**	-.473**	1		
Q	-.471	.390**	.401**	-.484**	-.227*	.428**	-.428**	-.283**	-.539**	-.494**	.402**	.461**	361**	1	
Inv	.499**	-.321**	.659**	.658**	.017	.662**	.136	.199*	.189	.649**	.484**	.453**	-.417**	.355**	1

Source: SPSS Version 23 Output, 2023

4.4. Regression Analysis

Regression has used in this research to determine the relationship between one or more independent variables (management support, economy etc...) and a dependent variable (information system security investment). The resulting model helps predict how changes in the independent variables affect the dependent variable. The regression coefficient(s) represent the change in the dependent variable resulting from a change in the independent variable. A positive coefficient indicates that an increase in the independent variable leads to an increase in the dependent variable, while a negative coefficient indicates the opposite and the size of the coefficient represents the magnitude of the effect. Whereas R-squared value provides an overall measure of the model's fit. This value ranges from 0-1, with a value closer to 1 indicating a better fit. A high R-squared value indicates that the independent variable(s) explain a significant portion of the variation in the dependent variable.

Table 4.19: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.862[a]	.743	.693	.321

a. Predictors: (Constant), Q, Ex, F, MP, VM, OS, A, D, L, BC, MS, R, E, FG

Source: SPSS Version 23 Output, 2023

As per the finding of the study which is shown in the table 2, the result of regression analysis multiple coefficients of determination or R square (R^2=0.743) exhibited that 74.3% of variations in the measurement of Information system security Investment can be explained by Technological, Organizational and environmental factors characterized by Lack of Management Support, Misperception, Economy, Legal and Regulatory framework, Lack of Experience on security incident, Awareness, Decision support process, Lack of financial models, organization culture, risk Assessment, considering existing organization infrastructure, Not considering future growth, lack of vendor management and lack of quality of information system security solutions. Whereas the remaining 25.7 % is explained by other variables that are not part of this model. There are several other factors that may be suspected to constitute the remaining 25.7% such as other factors which were excluded from the scope of this study.

4.5. The effect of predicted variables on information system security investment (ANOVA)

In regression analysis, ANOVA (analysis of variance) is used to determine whether there is a significant difference between the means of two or more groups. The interpretation of the regression analysis in multiple linear regressions is done by examining the estimated coefficients of each independent variable. The regression coefficients indicate the strength and the direction of the relationship between the dependent variable and each independent variable. When the regression coefficient is positive, it suggests that an increase in the independent variable will lead to an increase in the dependent variable. On the other hand, when the regression coefficient is negative, it suggests that an increase in the independent variable will lead to a decrease in the dependent variable.

Table 4.20: The effect of predicted variables on Investment (ANOVA)

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	21.233	14	1.570	14.700	.000[b]
Residual	7.325	71	.103		
Total	28.558	85			
a. Dependent Variable: Inv					
b. Predictors: (Constant), Q, Ex, F, MP, VM, OS, A, D, L, BC, MS, R, E, FG					

Source: SPSS Version 23 Output, 2023

Moreover, the p-value of each independent variable in the regression analysis results is also important. If the p-value is less than the chosen level of significance (usually 0.05), the independent variable is said to be statistically significant in explaining the variation in the dependent variable. As the ANOVA table , the statistical significance result indicates a value of .000 which shows the value of $p < 005$ which shows a quite good degree of prediction.

Table 4.21: Regression analysis summary of predictor variables

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	5.892	.680		8.662	.000
Q	.054	.056	.085	.965	.338
MS	.139	.061	.254	2.293	.025
MP	-.091	.058	-.124	-1.571	.121
E	.204	.073	.331	2.806	.004
L	.171	.075	.274	2.280	.026
Ex	.092	.048	.141	1.920	.059
A	.255	.065	.416	3.939	.000
D	.215	.071	.306	3.048	.003
F	.052	.063	.083	.822	.414
BC	.139	.071	.219	1.952	.004
R	.238	.075	.398	3.188	.002
OS	.129	.083	.176	1.558	.124
FG	.267	.088	.433	3.050	.003
VM	-.072	.056	-.103	-1.292	.201

a. Dependent Variable: Inv

Source: SPSS Version 23 Output, 2023

Another parameter this study aimed to identify is that which of the variables contributed the most to prediction of the dependent variable. This can be investigated through Standardized coefficient Beta. The importance of standardized coefficients in interpreting regression models is that beta coefficients represent the change in the outcome variable associated with a one-unit increase in the predictor variable, holding all other predictors constant. The standardized coefficient beta also indicates the magnitude and direction of the effect of an independent variable on the dependent variable while keeping all other independent variables constant. Beta values range from -1 to +1, with negative values suggesting an inverse relationship and positive values implying a positive relationship between the two variables.

According to the findings, From the Technological Context, the findings quality information system security solution has coefficient of (β=.085, p = .338). The significance level (p>0.05) therefore, the null hypothesis, *H_{01}: quality information system security solution has no effect on Information System security Investment, is not rejected*. This means, there is no significant relationship between quality of information system solutions and information system security investment.

According to the findings, From the Organizational Context, Management support has coefficient of (β = .254, p = .025). As a result of the significance level (p<0.05), the null hypothesis *H_{02}: Management support has no positive and significant impact on Information System Security Investment* is rejected. This means, there is a significant relationship between management support and information system security investment. Misperception of Information System Security and Information System Security Investment has a coefficient (β=-.-124, p = .121). As a result of the significance level (p>0.05), the null hypothesis *H_{03}*: *misperception has no significant effect on Information System security Investment is not rejected*. Thus, Misperception has no significant impact on information security investment. From the findings indicates, Economy has a coefficient, (β=.331, p = .004). As a result of the significance level (p<0.05), the null hypothesis *H_{04}: Economy has no positive effect on Information System security Investment* is rejected. Thus, there is a significant relationship between Economy and information system security investment. Based on the findings Information system security Awareness has a Coefficient of (β= .416, p = .000). As a result of the significance level (p<0.05), the null hypothesis *H_{05}: Information system security Awareness has no significant effect on Information System security Investment is rejected.* Thus, there is a significant relationship between Awareness and information system security investment. From the Findings, Decision Support process has a Coefficient of (β=.306, p = .003). As the result of the significance level (p<0.05). The null hypothesis is *H_{06}*: *Decision Support process has no significant effect on Information System security Investment* is rejected. Therefore, Decision Support process has a positive relationship with information system security investment. From the findings considering the existing organization Infrastructure has coefficient of (β=.176, p = .124). The significance level is greater than (p>0.05). Therefore, the null hypothesis *H_{07}*: *considering the existing organization has no significant impact on Information System security Investment is not rejected.* From the findings Risk Assessment has Coefficient of (β=.398, p = .002). The significance level is less than (p< 0.05). Therefore, the null hypothesis *H_{08}*: *Risk Assessment has no positive effect on*

Information System security Investment is rejected. This shows Risk Assessment has a positive significant impact on information system security investment. Considering Future Growth has a Coefficient of (β=.433, p = .003). The significance level is less than (p<0.05). Therefore, the null hypothesis H_{09}: *considering Future Growth has no positive significant effect on Information System security Investment is rejected.* In addition, coefficient (β=.353) shows, considering Future Growth has a positive relation with information system security investment. From the findings organization culture has Coefficient of (β=.219, p = .004). The significance level is less than (p<0.05). Therefore, the null hypothesis H_{010}*: organization culture has no positive significant effect on Information System security Investment* is rejected. This shows Organization Culture has a positive significant effect on information system security investment.

According to the findings, Environmental Context shows, Legal and regulatory Frameworks has a Coefficient of (β=.274, p = .026). The significance level is less than (p<0.05), Therefore, the null hypothesis H_{011}*: a legal and regulatory framework has no positive effect on Information System security Investment* is rejected. This shows Legal and regulatory framework has a positive significant effect on information system security investment. From the findings vendor involvement has a coefficient of (β=-.103, p = .201). The significance level (p>0.05). Therefore, the null hypothesis *is* H_{012}*: vendor involvement has no positive significant effect on Information System security Investment is not rejected.* With respect to this, Vendor involvement has no significant effect on information security investment. From the findings, financial models has a Coefficient of (β=-.083, p = .414). The significance level (p>0.05). Therefore, the null hypothesis $H_{013:}$ *financial models have no positive effect on Information System security Investment* is not rejected. Thus, Financial Models has no significant effect on information security investment. From the findings Experience on security incident has a Coefficient of (β=.141, p = .059). The significance level (p>0.05). Therefore, the null hypothesis $H_{014:}$ Experience on security Incidents has no positive significant effect on Information System security Investment is not rejected. Thus, Experience on security incident has no significant effect on information security investment.

CHAPTER 5: SUMMARY OF FINDINGS, DISCUSSIONS, CONCLUSION, AND RECOMMENDATION

The purpose of this this research was to identify the factors that influence information system security investment decisions. The results of the study were presented and discussed in the previous chapter. This Chapter summarizes the findings and draws conclusions. Recommendations for action are made and areas for further research are identified.

5.1. Summary of Major findings

This Study investigates the factors influencing information system security investment in selected public organizations using TOE framework which includes the technological, organizational and environmental factors. Data collected through the questionnaire was analyzed by descriptive analysis, correlation and multiple regressions. Finally, the researcher comes up with the following key summary findings. The first aim of the study was to identify factors affecting information system security investment in public organizations using TOE framework. In addition, The Research determines the significance level of each factor affecting information system security investment. Based on the TOE model, the variables involved in the current research were defined as technological, environmental and organizational factor. Based on the findings, Quality of information system security categorized under technological factors has no significant relationship with information system security investment. Besides, Top management support, Economy, Awareness, decision support process, and Risk assessment, future growth and organization information security culture, categorized under organizational factors has a significantly affect information system security investment. An environmental factor which includes Legal and Regulatory Frameworks has significantly affect information system security investment.

5.2. Discussions

The first aim of the study is to determine factors affecting information system security investment.

Research Question #1: *What are the factors that influence information system security investment on selected public organizations in Ethiopia*?

Based on the TOE model, the variables involved in the current research were defined as technological, environmental and organizational, Thus, Quality of information system

security is categorized under technological factors which affect information system security investment. Besides, Top management support, Misperception of Information system security, Economy, Awareness, decision support process, considering of organization infrastructure and Risk assessment, future growth and organization security culture are categorized under organizational factors affecting information system security. Environmental factors Includes Legal and Regulatory Frameworks, vendor involvement, financial models and experience of security incident.

The Second objective of the research was to address how those factors affect information system security investment and determine their significance level of each factor on information system security investment.

Research Question #2: How those factors affect information system security investment in public organization in Ethiopia?

Based on the findings, From Technological Context. Quality of information security solutions has no significant impact. However other previous studies confirmed quality solutions has a significant impact on investment. According to (lee *et al.,* 2018), the complexity of security solutions influence peoples to use and invest in information security technology. With respect to (Hasani *et al.,* 2023)research findings shows that technology quality, which includes compatibility, trial ability, usability, is a significant factor which affects the adoption of cyber security technologies. From the Findings in Organizational Context, Management Support has a positive significant effect on information system security investment. Previous research by (Hsu *et al.,* 2012) and (Daud *et al.,* 2018) investigated the effects of top management support on security innovation, effectiveness, and compliance and discovered that organizations should pay special attention to top management's commitment to promoting security technology adoption. According to (Ključnikov *et al.,* 2019), states, organizational top management support has the major effect on information security since top management support directly oversees all processes inside the organization, therefore, a lack of top management support has substantial impact on investment in information systems security. Senior management should set a good example (in the organization) by guaranteeing effective training and awareness programs, as well as positively enhance their security behaviour (Alhogail *et al.,* 2015).

From the findings, Misperception has no significant impact on information system security investment. However, as confirmed by other study (Ng *et al.,* 2013) discussed misperception of a security has a series of impact on an organization's decision towards information security investment. According to the findings, Economy has a significant positive impact on information system security investment. As the organization budget allocation to information security increase, the effectiveness on decision of information system security increase (Toivanen *et al.,* 2015). As (Kirubel, 2022) states, Sufficient budget has an effect on information system security investment. From the findings, Awareness has a significant impact on information system security investment. With respect to (carias *et al.,* 2018) confirmed, the increase in organization awareness is the more investment in technical security. From the findings, Risk assessment has a significant positive impact on information system security investment. As (Tovinen, 2015) discussed the entire decision of cyber risk management influence the investment decision. From the findings, decision support process has positive significant impact on information system security investment. With respect to (Schatz and Bashroush, 2018) sates Decision support mechanisms and information based on evidence have a major impact on information system security investment. From the findings, considering organizational infrastructure has no significant impact on information security investment, Although, the findings shows no significance, other researches confirmed Considering organization structure has an effect on security investment (Kirubel, 2022). In addition, considering organizational architecture, best practices, standards, and awareness are key in structuring the processes of strengthening an organization's information security, all of which have a direct impact on the organization's information security decisions making. (Diesch *et al.,* 2020). From the findings, considering future growth has a significant impact on information system security investment, other studies like (Kirubel 2022), (Eric 2018) confirmed determining long and short term growth has a significant effect on information system security investment. From the findings, Organization security culture has a positive significant impact on information system security investment. The acknowledgment of information security importance is considered as the major driving factor on information security investments. As (De Vries, 2017) states organizational characteristics such as business type, organizational size, culture has a substantial influence on the investment behaviour. With respect to (Parsons *et al.,* 2015) improving the organizational information security culture within an organization should improve compliance with policy and

procedures, and has a relationship with enhancing employees' information security decision making.

Based on the findings, On Environmental Context, legal and regulatory framework has a positive significant impact on information system security investment decision. From the other study findings, organization's information security maturity greatly depends on the effectiveness of security governance structures which is the fundamental variable needed for business enablement as well as running security programs in the organization (Edwards, 2018) As (Weishäupl *et al.,* 2018) states, the primary external drivers for decisions to invest in information system security investment are legal frameworks, rules and acts that place a heavy burden on organization. From the findings vendor involvement has no significant effect on information system security investment. Although, the findings show no significance, other studies find confirms vendor management has an effect on information system security investment. As (Kirubel, 2022) discussed vendor involvement has a huge impact in investment on information system security solutions. From the study findings, Experience on security has no significant impact on information system security investment However, although this research shows this finding, according to prior research findings. Many businesses do not currently set budgets because there haven't been any security problems, which mean that experience in information security affects security expenditure (lee *et al.,* 2018). Security incidents are a major motivator for security investment (Schatz and Bashroush 2018). From the findings, financial evaluation models analysis has no significant impact on information system security investment. Although, these study findings show this result, different studies stated finical models have a significant impact on information system security investment. Economic models of information security investment suggest estimating cost and benefit to make an information security investment decision (Shawo *et al,* 2019). In addition the assessment of Financial analyses and determining the assets, threats, vulnerabilities of information systems and has an impact for the essential security investment (Weishäupl *et al.,* 2018).

The Third objective of this study deals on how can information system security investments guided.

Research Question #3 how can information system security guided?

This research identifies the factors that influence information system investment and their level of significance. By becoming aware of these influencing factors, organizations can

improve their operations and contribute to the effective decision-making process regarding with investments. Meanwhile, organization's information security would gain prominence. According to the findings, information system security investment could be guide by the following measure. The Suggestions are based on the findings from the quantitative study. The outcome of the quantitative study helps to determine the significant level of effect of each factor that affects information system security investment. Due to this, the following improvement points are provided.

- Top management support improves the investment in information system security. Because senior management plays an important function in an organization and can emphasize different decisions. It should treat information system security investment as a vital business component. The commitment and Support of the management can guide and improve the information system security investment.
- The organization should also provide training to raise awareness about the security. Enhancement of information system security training raises the level of knowledge among management and key decision makers. As a result, it can increase intention of spending in information system security. Furthermore, training can assist both professionals and non-experts eliminate their biases.
- Organizations must create security controls, policies, and frameworks in order to maintain their spending in security. The better acknowledgment of standards on security, it leads to better security investment and loss of cyber disaster.
- Organizations should use decision process approaches when investing in information system security measures to help them calculate the security return on investment with respect to the mission of the organization. Once organization acknowledges, organization will spend money on security.
- Organizations can influence organizational culture and attitudes towards information security by establishing acknowledgment programs on information security investment by advocating the relevance of information security. Public institutions may have utilized sophisticated solutions besides strategies to secure themselves. However, it is important to remember that humans remain the weakest link. Organizational culture and attitudes towards positive information security thinking can be achieved by making employees know the importance of security of information. The organization should have aligned the investment with the organization mission and the organization should do periodic risk assessment and prioritization on security investment.

5.3. Conclusion of the Study

Investing in security is becoming increasingly important. However there are different factors which influence the spending on information system security. The research determines the variables which affect information system security investment using TOE model. In addition, the study measures each variable which has an effect of in security investment. The study have a major contribution to acknowledge about security and assist decision makers on decision making process and it provide a clear view of factors that have an influence on the decision-making process regarding to spending in information security. Identifying the factors that influence security investment decisions will assist decision makers to drive better cyber-security investment decision-making in a proper manner. Different prior literatures reviewed and data was collected using questionnaire to identify the factors affecting investment decisions on information security investment based on different prior researches. Conceptual framework was developed and served as a blueprint to conduct the study.

The TOE factors classified as technology, organization and environmental factors has been assessed. Based on the study findings, Although The technological factors, quality of information system security solutions doesn't show the significant impact on information system security investment, There are different researches confirmed it has an effect on investment. The organizational factors including, management support, economy, awareness, decision support process, risk assessment, future growth and organization information security culture has a significant impact on information security investment. According to the result findings, Environmental factors which includes legal and regulatory framework, has an impact on security investment. To make effective information system security investment the top management and decision makers should a provide an adequate resources, prepare trainings, building organizational culture among the employees, taking risk assessment, enforcing laws, decision support process and developing long term goal align with the organization mission. Furthermore, this research serves as a guide for decision makers to assist in decision making with regard to information system security investment. The researchers believed that, this research fills the theoretical gap and could be roadmap for further researchers.

5.4. Recommendations of the Study

According to previous outcome of the study, the researcher recommends those points for management intervention to help improve their security solution investment.

- Prior to investing in a security solution, all top managers, IT security managers, team leaders, and security team members should able to deploy frameworks, laws and that aligned with the organization mission. Moreover, it should be assist by the decision makers.
- Organizations need to implement security controls, polices and frameworks and use them to protect information security it should be supported by the management, and aligned with business objectives.
- public organizations should have an extensive understanding of the elements that impact security solution selection
- It is highly recommended to increase in the training level of information system Organizations must develop security controls, policies, and frameworks to ensure information security. These measures must be facilitated by management and corresponded with business objectives.
- Organization should invest in the capacity building and knowledge of their teams.

5.5. Research Limitation & Suggestion for Future Research

5.5.1. Limitation of the study

This study had several limitations. First, like any other sort of research, the sample size may effect or influence the conclusions. This research only includes eight government organizations in Ethiopia. As a result, it is inapplicable to other organizations or states. The study used only TOE based model and investigates each characteristics which impact security investment.

5.5.2. Suggestions for future research

This research found out factors that influence investment decisions on information security investment, and the researchers still believes that there are more factors that influence security investment which should be researched. Furthermore, this study research focused on Selected Ethiopian public organizations, it would be excellent if future researchers included non-governmental organizations, and so on, and this research could be a precedent for future researches.

REFERENCES

ABD ALWALI, L. U. T. F. I. (2017). Antecedents and impact of AIS usage amongst Jordanian smes: moderating effects of environmental uncertainty and firm size.

Abed, S. S. (2020). Social commerce adoption using TOE framework: An empirical investigation of Saudi Arabian SMEs. *International Journal of Information Management*, *53*, 102118. Https://doi.org/10.1016/j.ijinfomgt.2020.102118

Abomhara M. & G. M. Koien (2015) Cyber-security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber-security, Vol. 4, 65–88.

Aghaunor, G., & Okojie, B. E. (2022). Factors Influencing the Implementation of Information Security Risk Management: A case study of Nigerian Commercial Banks.

Aigbovo, O., & Ilaboya, O. J. (2019). Does behavioural biases influences individual investment decisions. *Management Science Review*, *10*(1), 68-89.

Ajzen I (1991) The Theory of planned behavior. Organization Behavior Human Decision process 50(2):179-211

Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. Computers & Security, 74, 323-339

Al-Dhahri, S., Al-Sart, M., & Abdul Aziz, A. (2017, January). Information Security Management System. Retrieved January 9, 2023, from Https://www.academia.edu/72791819/Information_Security_Management_System

Alhogail, A., Mirza, A., & Bakry, S. H. (2015). A Comprehensive human factor framework for information security in organizations. Journal of Theoretical and Applied Information Technology, 78(2), 201-211.

Alqahtani, F. H. (2017). Developing an information security policy: A case study approach. 4th Information Systems International Conference (pp. 691-697). Bali, ISICO

Aregahegn, W. (2022, June 16). INSA Saves 1.4 Billion Birr by Thwarting 97 Percent of Cyber Attacks. Welcome to Fana Broadcasting Corporate S.C. Https://www.fanabc.com/english/insa-saves-1-4-billion-birr-by-thwarting-97-percent-of-cyber-attacks/

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, 147, 113580. Https://doi.org/10.1016/j.dss.2021.113580

Au Y, Zafar H (2008) A multi-country assessment of mobile payment adoption. No. Wp# 0055IS-296-2008, Texas. Available at: Https://api.semanticscholar.org/CorpusID:35575634

Autry C, Grawe S, Daugherty P, Richey R (2010) The effects of technological turbulence and breadth on supply chain technology acceptance and adoption. J Oper Manag 28(6):522–536

Avci, Onur & Ozbulut, Osman. (2018). Threat and Vulnerability Risk Assessment for Existing Subway Stations: A Simplified Approach. *Case Studies on Transport Policy*. Https://doi.org/10.1016/j.cstp.2018.08.005.

Bacon, J. 1994. "Why companies invest in information technology ?" MIS Quarterly. September, pp. 335-354

Benaroch, M. (2018). Real Options Models for Proactive Uncertainty-Reducing Mitigations and Applications in Cyber security Investment Decision Making. *Information Systems Research*, 29(2), 315–340. Https://doi.org/10.1287/isre.2017.0714

Bogner A, Littig B, Menz W (2009) Introduction: Expert interviews – An introduction to a new methodo?logical debate. In: Bogner A, Littig B, Menz W

Böhme, R. (2010, November). Security metrics and security investment models. In *International Workshop on Security* (pp. 10-24). Berlin, Heidelberg: Springer Berlin Heidelberg.

Bojanc, R., & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. International Journal of Information Management, 28(5), 413-422. doi: 10.1016/j.ijinfomgt.2008.02.002

Bryan, J. D., & Zuva, T. (2021). A Review on TAM and TOE Framework Progression and How These Models Integrate. Advances in Science, Technology and Engineering systems Journal, 6(3), 137-145. https://doi.org/10.25046/aj060316

Caffaro F, Micheletti Cremasco M, Roccato M, Cavallo E (2020) Drivers of farmers' intention to adopt technological innovations in Italy: the role of information sources, perceived usefulness, and perceived ease of use. J Rural Stud 76:264–271

Cao, Y., Ajjan, H., Hong, P., & Le, T. (2018). Using social media for competitive business outcomes: An empirical study of companies in China. *Journal of Advances in Management Research*, *15*(2), 211-235.

Carías, J. F., Labaka, L., Sarriegi, J. M., & Hernantes, J. (2019). Defining a Cyber Resilience Investment Strategy in an Industrial Internet of Things Context. *Sensors*, 19(1).Https://doi.org/10.3390/s19010138

Carmines, E. G., & Zeller, R. A. (1979). Reliability and validity assessment. Sage Publications.

Cavana, R., Delahaye, B., & Sekerean, U. (2001). *Applied business research*: Qualitative and quantitative methods. John Wiley & Sons.

Chai, S., Kim, M., & Rao, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems*, 50(4), 651–661. Https://doi.org/10.1016/j.dss.2010.08.017

Charlton, A. B., & Cornwell, T. B. (2019). Authenticity in horizontal marketing partnerships: A better measure of brand compatibility. *Journal of Business Research*, *100*, 279-298.

Chatzoglou P, Chatzoudes D,D ragdidis L, Symeonidis S(2017) Examining the critical success factor for ERP implementation: Explanatory study conducted in SMEs.

Cheng, L. et al., (2013). Understanding the Violation of IS Security Policy in Organizations: An Integrated Model Based on Social Control and Deterrence Theory. *Computers & Security*, 39:447–459

Choi, M., Lee, J., & Hwang, K. (2018, May 14). Information Systems Security (ISS) of E-Government for Sustainability: A Dual Path Model of ISS Influenced by Institutional Isomorphism. *Sustainability*, *10*(5), 1555. Https://doi.org/10.3390/su10051555

Chu, A. M., & So, M. K. (2020) Organizational Information security management for sustainable information systems: *An unethical employee information security behavior perspective. Sustainability*, 12(8), 3163

Creswell, J. (2014). *Research design: Qualitative, quantitative and mixed method approaches* (4th Ed.). SAGE publications, Thousand Oaks, California

Cybercrime mag. (2019, June 10). Global cyber security spending predicted to exceed $1 trillion from 2017-2021. Cybercrime Magazine. Https://cybersecurityventures.com/cybersecurity-market-report/

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020, May). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713. Https://doi.org/10.1016/j.cose.2020.101713

Daud, M., Rasiah, R., George, M., Asirvatham, D., & Thangiah, G. (2018). Bridging the gap between organisational practices and cyber security compliance: can cooperation promote compliance in organisations. *International Journal of Business & Society*, *19*(1).

DAVIDAVIČIENĖ, V., RAUDELIŪNIENĖ, J., TVARONAVIČIENĖ, M., KAUŠINIS, J. 2019. The importance of security aspects in consumer preferences in electronic environment. Journal of Security and Sustainability Issues, 8(3), 399-411. Http://doi.org/10.9770/jssi.2019.8.3(9)

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.

De Vries, J. (2017). What drives cybersecurity investment?: organizational factors and perspectives from decision-makers.

De Vaus, D., & de Vaus, D, (2013). *Survey in social research. Routledge*,2013

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human factors in phishing attacks: a systematic literature review. *ACM Computing Surveys (CSUR)*, *54*(8), 1-35.

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, *92*, 101747.

Digital Ethiopia. (2022). Retrieved June 13, 2023, from https://mint.gov.et/wp-content/uploads/2022/01/Summary_of_Digital_Strategy_Final_English1.pdf

Dor, D., & Elovici, Y. (2016). A model of the information security investment decision-making process. *Computers & Security*, 63, 1–13. Https://doi.org/10.1016/j.cose.2016.09.006

Edwards, M. M. (2018). *Identifying factors contributing towards information security maturity in an organization* (Doctoral dissertation, Nova Southeastern University).

Ekelund, S., & Iskoujina, Z. (2019). Cybersecurity economics–balancing operational security spending. *Information Technology & People*, *32*(5), 1318-1342.

Eric, D. (2018). How to Choose the Best Data Security Solution for Your Enterprise. Https://www.compuquip.com/blog/data-security-solution

Ernest Chang, S., Ho, C.B., 2006. Organizational factors to the effectiveness of implementing information security management. Indus. Manag. Data Syst. 106 (3), 345–361. doi:10.1108/02635570610653498.

Ethiopia Digital Strategy 2020.pdf. (n.d.).

Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics*, *3*(5), 97

Fedele, A., & Roner, C. (2022). Dangerous games: A literature review on cybersecurity investments. *Journal of Economic Surveys*. Https://onlinelibrary.wiley.com/doi/abs/10.1111/joes.12456

Fenz, S., Ekelhart, A., & Neubauer, T. (2011). Information Security Risk Management: In Which Security Solutions Is It Worth Investing? *Communications of the Association for Information Systems*, 28(1), 22. Https://doi.org/10.17705/1CAIS.02822

Fielder, A., König, S., Panaousis, E., Schauer, S., & Rass, S. (2018). Risk Assessment Uncertainties in Cybersecurity Investments. *Games*, 9(2), 34. Https://doi.org/10.3390/g9020034

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision support systems*, *86*, 13-23.

Fields, Z., Fields, Z., & Patrick, H. (2016). Security- information flow in the south african public sector. Journal of Information Warfare, 15(4), 68-85.

Geric, Sandro & Hutinski, Željko. (2007). Information system security threats classifications. *Journal of Information and Organizational Sciences.*

Getnet, G. (2020) Assesement of Information Systems Security Mangement in Selected Public Organizations in Ethiopia: A Gap Analysis, Addis Ababa University, Ethiopia

Gliem, J. A., & Gliem, R. R. (2003). *Calculating, interpreting, and reporting cronbach's alpha reliability coefficient for likert-type scales.* Http://scholarworks.iupui.edu/handle/1805/344

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, 1(1), 3–17. Https://doi.org/10.1093/cybsec/tyv011

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015).investing in cyber security:Insights frim the Gordon-Loeb model. Journal of information security,7(02),49

Govender, S. G., Loock, M., & Kritzinger, E. (2018). Enhancing Information Security Culture to Reduce Information Security Cost: A Proposed Framework. *Cyber space Safety and Security*, 281–290. Https://doi.org/10.1007/978-3-030-01689-0_22

Hall, J. H., Sarkani, S., & Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security*, 19(3), 155–176. Https://doi.org/10.1108/09685221111153546

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics*, *3*(5), 97

Hashim, R., & Razali, R. (2019). Contributing Factors for Successful Information Security Management Implementation: A Conceptual Model. *International Journal of Innovative Technology and Exploring Engineering*, *9*(2), 4491-4499.

Heale, R., & Twycross, A. (2015). Validity and reliability in quantitative studies. *Evidence-Based Nursing*, *18*(3), 66–67. Https://doi.org/10.1136/eb-2015-102129

Home - En - INSA. (n.d.). Retrieved June 15, 2023, from https://www.insa.gov.et/web/en Https://doi:10.13052/jcsm2245-1439.414

Ifinedo, P. (2013). Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialization, Influence, and Cognition. *Information & Management*, Http://dx.doi.org/10.1016/j.im.2013.10.001

Ioannidis, C., Pym, D., & Williams, J. (2016). Is public co-ordination of investment in information security desirable?. *Journal of Information Security, 7*, 60-80.

ISO/IEC 27002 (2005) ISO/IEC 27002:2005, Information technology - Security techniques - Code of practice for information security management. International Organization for Standardization (ISO) and International Electrotechnical Commission.

Jabangwe, R., & Nguyen-Duc, A. (2020). A SIoT framework: Towards an approach for early identification of security requirements for internet-of-things appkications. *E-informatica Software Engineering Journal*, 14(1).

Jeong, C. Y., Lee, S.-Y. T., & Lim, J.-H. (2019). Information security breaches and IT security investments: Impacts on competitors. Information & Management, 56(5), 681–695. Https://doi.org/10.1016/j.im.2018.11.003

Kagwiria, C. (2020). Cyber Security Skills Gap in Africa. Nairobi: AFRALI

Kamiya, S., Kang, J. K., J., Milidonis, A., &Stulz, R. M. (2021). Risk management, Firm reputation, and the impact of successful cyber-attacks on target firms. Journal of financial Economics, 139(3), 719-749

Karjalainen, M., Siponen, M., Kohli, R. & Shao, X. 2014. "What's in it for me ? A Stakeholder Theory perspective on Information Technology Security Investment," *Completed Research Paper*. pp. 1-30.

Kayworth, T., Whitten, D. 2010. Effective Information Security Requires a Balance of Social and Technology Factors, In: MIS Quarterly Executive, 2010. ISSN 1540-1960,

Kazemi. 2012. Evaluation of information security management system success factors: Case study of Municipal organization. *AFRICAN JOURNAL OF BUSINESS MANAGEMENT, 6*(14). Https://doi.org/10.5897/ajbm11.2323

Kazemi.M., Khajoueil, H., NasrabaadiI, H. 2012. Evaluation of information security management system success factors: Case study of Municipal organization. In: African Journal of Business Management, 2012, roč. 6, č. 14, s. 4982-4989. ISSN 1993-8233

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021, July). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267. Https://doi.org/10.1016/j.cose.2021.102267

Kim, Y., & Kim, B. (2021). The effective factors on continuity of corporate information security management: Based on TOE framework. *Information*, 12(11), 446

Kirubel M, (2022) Factors Influencing Information Security Investments in the Ethiopian Banking Sector: Towards an Evaluation Framework, Addis Ababa University

Ključnikov, A., Mura, L., & Sklenar, D. (2019). Information security management in SMEs: factors of success. *Entrepreneurship and sustainability issues, 6(40, 2081.*

Kothari, C. (2004). *Research methodology: Methods and* techniques (2nd ed). New Delhi: New age international publisher.

Laudon,K. C., & Laudon, J. P. (2004). *Management information Systems: Managing the digital firm*. Pearson Education

Laurell, C., Sandström, C., Berthold, A., & Larsson, D. (2019). Exploring barriers to adoption of Virtual Reality through Social Media Analytics and Machine Learning–An assessment of technology, network, price and trialability. *Journal of Business Research*, *100*, 469-474.

Lavrov, E. A., Zolkin, A. L., Aygumov, T. G., Chistyakov, M. S., & Akhmetov, I. V. (2021, February 1). Analysis of information security issues in corporate computer networks. *IOP Conference Series: Materials Science and Engineering*, *1047*(1), 012117. Https://doi.org/10.1088/1757-899x/1047/1/012117

Lee, H. J., Roh, E. H., & Han, K. S. (2018). A study on factors of information security investment in the fourth industrial revolution. International Journal of Advanced Science and Technology, 111, 157–174. Https://doi.org/10.14257/ijast.2018.111.14

Lee, I. (2021). Cyber security: Risk management framework and investment cost analysis. *Business Horizons, 64*(5), 659-671.

Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. *Journal of Entrepreneurship and Sustainability Issues*, 4(4), 559–573. Https://doi.org/10.9770/jesi.2017.4.4(12)

Liu, D., Ji, Y., and Mookerjee, V. 2011. "Knowledge Sharing and Investment Decisions in Information Security," Decision Support Systems (52 :1), pp. 95- 107.

Lopes, I., & Oliveira, P. (2015). Implementation of Information Systems Security Policies:A Survey in Small and Medium Sized Enterprises . Bragança, Portugal : Springer International Publishing

Lundgren, B., & Möller, N. (2017). Defining Information Security. *Science and Engineering Ethics, 25*(3), 1-8

Maarop, K. Thamadaran, G., N., Samy, A., Azmi, O.,Mohd-Yusof, A., Azizan, ―Information Security Management System Implementation Success Factors: A Review‖, Advanced Science Letter, Vol. 22, No. 10, pp. 3023-3026, 2015

Mazzoccoli, A., & Naldi, M. (2020). Robustness of Optimal Investment Decisions in Mixed Insurance/Investment Cyber Risk Management. Risk Analysis: An Official Publication of the Society for Risk Analysis, 40(3), 550–564. Https://doi.org/10.1111/risa.13416

Ministry of Education Ethiopia. (n.d.). Ministry of Education. Retrieved June 14, 2023, from Https://moe.gov.et/

Mithas, S., Tafti, A., Bardan, I., and Goh, J. M. 2012. "Information Technology and Firm Profitability : Mechnanisms and Empirical Evidence", MIS Quarterly, Vol 36 No.1, pp. 205-224. Mizzi, A. 2010. "Return on information sec

Mittal, P. (2020, October). Impact of digital capabilities and technology skills on effectiveness of government in public services. In *2020 International Conference on*

Data Analytics for Business and Industry: Way Towards a Sustainable Economy (ICDABI) (pp. 1-5). IEEE.

Montes, C., & Prabhu, J. (2023). Ethiopia Digital Connections for prosperity-ACCELERATING INNOVATIONS: DIGITAL ETHIOPIA 2025.

Moore, T., Pym, D. J., & Ioannidis, C. (2010). Economics of Information Security and Privacy. Springer US. Https://doi.org/10.1007/978-1-4419-6967-5

NCSI :: Ranking. (2022). https://ncsi.ega.ee/ncsi-index/

Nebyu E, (2018) Assessment of information security maturity level on Ethiopian Public Universities, Addis Ababa University

Ng, Z. X., Ahmad, A., & Maynard, S. B. (2013). Information Security Management: Factors that Influence Security Investments in SMES. Https://doi.org/10.4225/75/57b56667cd8e5

Nicho, M. (2018). A process model for implementing information systems security governance. *Information & Computer Security*.

Nieles, M., Dempsey, K., & Yan Pillitteri, V. (2017). An Introduction to Information Security. *NIST Special Publication* 800-12 *Revision* 1, 1–101. Https://doi.org/10.6028/NIST.SP.800-12r1

NIST. (2009). "Recommended Security Controls for Federal Information Systems and Organizations." from http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf

Nweke, L. O.(2017). Using the CIA and AAA models to explain cybersecurity activities. *PM World Journal*, 6(12),1-3

Obeidat I., & Mughaid A., (2019). Implementing Factors of Information Security in Governmental Organizations of Jordan. ICDS 2019: The Thirteenth International Conference on Digital Society and eGovernments

Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *Electronic journal of information systems evaluation*, *14*(1), pp110-121.

Olsina, L., Dieser, A., & Covella, G. (2014). Metrics and indicators as key organizational assets for ICT Security assessment. *In Emerging Trends in ICT Security* (pp.25-440. Morgan Kaufmann.

Oscarson, P.(2003).Information security fundamentals, graphical conceptualizations for understanding: Research group VITS, Department of Business Administrations, Economics. *Statics and Informatics, Orebro University, Sweden.*

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117-129.

Patino, S.,& Yoo, S. G. (2018, November). Study of the maturity of information security in public organizations of Ecuador. *In international conference on Technologies and innovation (pp.99-109). Springer, Chian*

Qadir, S., & Quadri, S. M. K. (2016) Information Availability : An insight into the most important Attribute of Information Security. *Journal of Information Security*,7(3), 185-194.

R.W. Rogers, "A protection motivation theory of fear appeals and attitude change", The journal of psychology, vol. 91, no. 1, (1975), pp. 93-114.

Rainer, R. K., & Prince, B. (2021). *Introduction to information systems*. *John Wiley & Sons.*

Rajnoha, R., Koraus, A., & Dobrovic, J. (2017). Information systems for sustainable performance of organizations. *Journal of Security and Sustainability Issue*s, 7(1), 167-179. Https://doi.org/10.9770/jssi.2017.6.1(14)

Reedy ,G. N., & Reddy,G. J. (2014). A study of cyber security challenges and its merging trends on latest technologies. *arXiv preprint arXic*:1402.1842.

Riolli, L., & Savicki, V. (2003). Information system organizational resilience. *Omega*, *31*(3), 227-233.

Rowe, B. R., & Gallaher, M. P. (2006, March). Private sector cyber security investment strategies: An empirical analysis. In *The fifth workshop on the economics of information security (WEIS06)*.

Sabherwal, R., Jeyaraj, A., & Chowa, C.(2006).Infomayion system success: individual and organizational determinants. Management science,52(12),1849-1864

Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., & Sookhak, M. (2019). Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Generation Computer Systems*, *97*, 587-597.

Safi, R. (2016). *Investment Decisions in Acquiring Information Security Measures: An Empirical Investigation* (Doctoral dissertation).

Safi, R., & Browne, G. (2015). Investment in Information Security Measures: A Behavioral Investigation.

Samimi (2020) Risk management in information technology."progress in chemical and biochemical research 3, no. 2(2020):130-134.

Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *information security technical report*, *15*(3), 112-133.

Schatz, D., & Bashroush, R. (2016, April 18). Economic valuation for information security investment: a systematic literature review. *Information Systems Frontiers*, *19*(5), 1205–1228. Https://doi.org/10.1007/s10796-016-9648-8

Schatz, D., & Bashroush, R. (2018, April). Corporate Information Security Investment Decisions. *International Journal of Enterprise Information Systems*, *14*(2), 1–20. Https://doi.org/10.4018/ijeis.2018040101

Shao, X., Siponen, M., & Pahnila, S. (2019, January). To calculate or to follow others: how do information security managers make investment decisions?. In *Proceedings of the 52nd Hawaii International Conference on System Sciences, January 8-11 2019, Grand Wailea, Maui*. Hawaii International Conference on System Sciences.

Shao,X., Siponen, M.,& Pahnila,S.(2019,January).

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014, March). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217–224. Https://doi.org/10.1016/j.im.2013.08.006

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225.

Spremić, & Šimunic. (2018). Cyber security challenges in digital economy. Proceedings of the World Congress of Neurological Surgery of the World Federation of Neurosurgical Societies. Http://www.iaeng.org/publication/WCE2018/WCE2018_pp341-346.pdf

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future generation computer systems*, *92*, 178-188.

Stair, R., & Reynolds,G.(2020). *Principles of information systems*.Cengage Learning

Taherdoost, H. (2016). Validity and reliability of the research instrument; How to test the validation of a questionnaire/survey in a research. *SSRN Electronic Journal*. Https://doi.org/10.2139/ssrn.3205040

Tasril, Virdyra & Ginting, Meiliyani & Mardiana, Mardiana & Siahaan, Andysah Putera Utama. (2017). Threats of Computer System and its Prevention. International Journal of Scientific Research in Science and Technology. 3. 448-451.

Temtim, A & Alpha T,(2021) Factors influencing information security compliance: an institutional perspective, , Addis Ababa University

Tewamba, H. N., Kamdjoug, J. R. K., Bitjoka,G. B., Wamaba, S. F., & Bahanag, N. N. M. (2019). Effects of information security management systems on firm performance. American Journal of operations and management and information systems, 4, 9-108. Https://doi.org/10.11648/j.ajomis.20190403.15

The National Information and Communication Technology Policy and Strategy. (2017). FDRE ICT policy and strategy. Retrieved June 13, 2023, from

Https://comesabusinesscouncil.org/wp-content/uploads/2020/04/6-ICT-Policy-and-Strategy.pdf

Toivanen, H. (2015). Case study of why information security investment fail? Https://jyx.jyu.fi/handle/123456789/46669

Tornatzky, L., & Fleischer, M. (1990). The process of technology innovation, Lexington, MA.

Tu, C. Z., Yuan, Y., Archer, N., Connelly, C. E. 2018. Strategic value alignment for information security management: a critical success factor analysis. In: *Information & Computer Security,* 2018. ISSN 2056-4961, roč. 26, č.2, s.150-170

V. Venkatesh, M. G. Morris, G. B. Davis and F. D Davis, "User acceptance of information technology: Toward a unified view", MIS quarterly, (2003), pp. 425-478.

Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J., & Botha, R. (2020). Information and Cyber Security: 19th International Conference, ISSA 2020, Pretoria, South Africa, August 25–26, 2020, Revised Selected Papers. *Springer Nature.* Https://play.google.com/store/books/details?id=bfYPEAAAQBAJ

Verbano, C., & Venturini,K. (2013). Managing Risks in SMEs: A literature review and Research Agenda. *Journal of Technology Management & Innovation*, 8, 186-197. Https://doi.org/10.4067/S0718-27242013000400017

Wallace, S., Green, K., Johnson, C., Cooper, J., & Gilstrap, C. (2021). An extended TOE Framework for cyber security Adoption Decisions. Communications of the association for information systems,47(2020),51

Wang, S. (2019). Integrated framework for information security investment and cyber insurance. *Pacific-basin Finance Journal*, *57*, 101173. https://doi.org/10.1016/j.pacfin.2019.101173

Watters, P. A., & Ziegler, J. (2016). Controlling information behaviour: The case for access control. Behaviour & Information Technology, 35(4), 268-276

Weishäupl, E., Yasasin, E., & Schryen, G. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security*, 77, 807–823. Https://doi.org/10.1016/j.cose.2018.02.001

Wessels, M., van den Brink, P., Verburgh, T., Cadet, B., & van Ruijven, T. (2021). Understanding incentives for cybersecurity investments: Development and application of a typology. *Digital Business*, 1(2), 100014. Https://doi.org/10.1016/j.digbus.2021.100014

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

Wolgemuth, J. R., & Agosto, V. (2019). Narrative research. *The black well encyclopedia of Sociology*, 1-3

Woretaw, A., Lessa, L., & Negash, S. (2019). Factors hindering full-fledged information security in banking sector in Ethiopia: Emphasis on information security culture.

Wu, Y., Feng, G., Wang, N., & Liang, H. (2015, September). Game of information security investment: Impact of attack types and network vulnerability. *Expert Systems With Applications*, *42*(15–16), 6132–6146. https://doi.org/10.1016/j.eswa.2015.03.033

Zhao, X., Ling, X., Andrew, B.W., 2013. Managing interdependent information security risks: cyber insurance, managed security services, and risk pooling arrangements. J. Manag. Inf. Syst. 30 (1), 123–152.

Zhuo, Yueran, "Managing Information Security Investments Under Uncertainty: Optimal Policies for Technology Investment and Information Sharing" (2019). Doctoral Dissertations. 1493. https://doi.org/10.7275/13455171 https://scholarworks.umass.edu/dissertations_2/1493

Zimmermann, M., Staicu, C. A., Tenny, C., & Pradel, M. (2019). Small world with high risks: A study of security threats in the npm ecosystem. In *28th USENIX Security Symposium (USENIX Security 19)* (pp. 995-1010).

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: a comparative study. *Journal of Computer Information Systems*, *62*(1), 82-97.

መግቢያ - ገቢዎች ሚኒስቴር. (n.d.). Retrieved June 15, 2023, from Http://www.mor.gov.et/

ANNEX

Addis Ababa University
College of Natural and Computational Sciences
School of Information Science

Introduction and Consent Form

Greetings

My Name is Eden Zewdie. I am doing my MSc in information systems at Addis Ababa University. Currently, I am conducting a Study entitled "FACTORS AFFECTING INFORMATION SYSTEM SECURITY INVESTMENT IN PUBLIC ORGANIZATIONS: A TOE BASED MODEL".

The research objective is to investigate the factors influencing information system security investment in Ethiopian public organizations. This research is expected to yield results that will provide a clear picture of the factors that influence the decision-making process for information system security investments and help in raising the level of understanding of security investment of decision-makers. Identifying the factors that influence security investment decision can help decision makers make better information system security investment decisions.

The interview questionnaire might take a maximum of 25 minutes. Your responses are extremely valuable to the outcome of this research. The results of the survey will be used for the purpose of academic research only. Your responses will be kept in strict confidentiality and would not affect anyone in any case.

You will kindly be asked to respond as soon as possible. Thank You in Advance.

If you have any questions or suggestions, please do not hesitate to contact me. Please use the following address

Email: - eden.zewdie@aau.edu.et

Cell phone: 0912774209

Questionnaire

Section I: PERSONAL DETAILS OF THE RESPONDENT		
INSTRUCTION: This part of the interview covers the personal and job related background information..		
S.N	Questions	Response
1.	Gender	Female ( ) male ( )
2.	Educational status	Certificate ( ) College Diploma ( ) Undergraduate ( ) Masters ( ) Ph.D. ( )
3.	Occupation status	ICT senior expert ( ) CIO( ) CSO( ) Director( ) CEO ( ) Department Head ( ) Manager( ) Chief administrative staff ( ) Others ( )
4.	Organization	AAU( ) FSC( ) MINT( ) MOE ( ) MOH ( ) MOR( ) MOT ( )

Section II Questions on factors affecting information system security investment

2.1 Management Support

Please rate/ circle your level of agreement with the following statements. The number indicates the following statement.

Directions: (1- strongly Disagree 2- Disagree 3-Neutral 4-Agree 5- Strongly agree)

S.N	Factors	Choose				
1.	Your organization's management demonstrates a commitment to enforcing information security polices across the organization.	1	2	3	4	5
2.	The management provides the essential facilities such as organizing training programs, or organizing security awareness workshops.	1	2	3	4	5
3.	The management provide the necessary budgets and resources for the successful implementation of the Information system security in the organization.	1	2	3	4	5
4.	The management prioritize information security just like other core business issues.	1	2	3	4	5

2.2 Misperception of information system security

Please rate/circle level of agreement with the following statements. The number indicates the following statement.

Directions: (1- strongly Disagree 2- Disagree 3-Neutral 4-Agree 5- Strongly agree)

S.N	Factors	Choose				
1.	Your organization does pay attention to external threats like viruses while underestimating the severity of internal problems	1	2	3	4	5
2.	Organization does perceive that they are to stop a concerted, premeditated attack.	1	2	3	4	5
3.	Your Organization does believe that investing in information systems security reduces an organization's productivity, profitability and business operations.	1	2	3	4	5

4.	Your organization does perceive the type of business they are in isn't going to be attacked.	1	2	3	4	5

2.3 Economy

Please rate/circle level of agreement to the following statements. The number indicates the following statement.

Directions: (1- strongly Disagree 2- Disagree 3-Neutral 4-Agree 5- Strongly agree)

S.N	Factors	Choose				
1.	Your organization does fund sufficient budget to spend in information systems security solutions	1	2	3	4	5
2.	Your organization is required to boost its budget if the organization damages are maximum or existent	1	2	3	4	5
3.	Your organization funds to hiring security specialists	1	2	3	4	5

2.4 Legal and regulatory framework

Please rate level of agreement to the following statements. The number indicates the following statement.

Directions: (1- strongly Disagree 2- Disagree 3-Neutral 4-Agree 5- Strongly agree)

S.N	Factors	Choose				
1.	Your organization utilizes international standard security frameworks.	1	2	3	4	5
2.	Your Organization has established defined rules and criteria's for assessing and prioritizing information system security investment	1	2	3	4	5
3.	Security policies are applied and ensures security.	1	2	3	4	5
4.	Your organization conduct audit and monitoring, impose penalties in case of security investment practices.	1	2	3	4	5

2.5 Experience on Security incidents

Please rate/circle level of agreement to the following statements. The number indicates the

following statement.

Directions: (1- strongly Disagree 2- Disagree 3-Neutral 4-Agree 5- Strongly agree)

S.N	Factors	Choose				
1.	Your organization considers internal security incidents as a critical security incident.	1	2	3	4	5
2.	Your Organization's budget for cyber protection is depending upon an incident of security event.	1	2	3	4	5
3.	Decision makers are not biased towards spending on information security measures.	1	2	3	4	5

2.6 Awareness

Please rate/circle your level of agreement with the following statements. The number indicates the following statement.

Directions: (1- strongly Disagree 2- Disagree 3-Neutral 4-Agree 5- Strongly agree)

S.N	Factors	Choose				
1.	Your organization management is technologically educated, and have a background on ICT	1	2	3	4	5
2.	There is no lack of knowledge and experience in information security among security personnel's	1	2	3	4	5
3.	Information system security decisions are made with considering the likelihood of occurrence, the probabilities of the outcomes, or the consequences.	1	2	3	4	5

2.7 Decision support process

Please rate/circle your level of agreement to the following statements. The number indicates the following statement.

Directions: (1- strongly Disagree 2- Disagree 3-Neutral 4-Agree 5- Strongly agree)

S.N	Factors	Choose

1.	There is Evidence based decision making procedures	1	2	3	4	5
2.	The decision to invest in information security relies on agreement between CISO and CIO with using proper multi-stakeholder decision models or approaches	1	2	3	4	5
3.	There is a common language due to that each stakeholders in the organization is eager to assist the one essential to himself/herself	1	2	3	4	5
4.	The organizational and psychological factors have no effect and no bias on organizational decision making	1	2	3	4	5

2.8 Financial valuation models

Please rate/circle level of agreement to the following statements. The number indicates the following statement.

Directions: (1- strongly Disagree 2- Disagree 3-Neutral 4-Agree 5- Strongly agree)

S.N	Factors	Choose				
1.	Your organization has capabilities to define the monetary value of investment	1	2	3	4	5
2.	Your organization has a method for predicting how much money would need to be invested before the organization experiencing cyber disaster	1	2	3	4	5
3.	Your organization is convinced and aware about the intangible costs and benefits of information security investments	1	2	3	4	5

2.9 organization information security culture

Please rate/circle your level of agreement with the following statements. The number indicates the following statement.

Directions: (1- strongly Disagree 2- Disagree 3-Neutral 4-Agree 5-

Strongly agree)

S.N	Factors	Choose				
1.	Based on the type of business the Organization has topic or mission for information security	1	2	3	4	5
2.	There exists awareness of the necessity of information security due to this there is IS specialist and IS department in the organization.	1	2	3	4	5
3.	There is cooperation between information security and business managers in aligning ISMS practices with organization mission					
4.	Organization does establishes an information security focus and emphasis norms among all employees	1	2	3	4	5

2.10 Risk assessment

Please rate/circle your level of agreement to the following statements. The number indicates the following statement.

Directions: (1- strongly Disagree 2- Disagree 3-Neutral 4-Agree 5- Strongly agree)

S.N	Factors	Choose				
1.	Your organization determines and classifies valuable assets and focus on how to protect them	1	2	3	4	5
2.	Your organization has an approach for recognizing and evaluating operational risks.	1	2	3	4	5
3.	Your organization has acknowledge of what it should be secure to and control strategies	1	2	3	4	5

2.11 consideration of the existing organizational structure

Please rate/circle your level of agreement with the following statements. The number indicates the following statement.

Directions: (1- strongly Disagree 2- Disagree 3-Neutral 4-Agree 5- Strongly agree)

S.N	Factors	Choose				
1.	Your organization use other organization prior experiences on information system security investment.	1	2	3	4	5

2.	Your organization does determine security solutions compatibility with the organization's infrastructure before investing.	1	2	3	4	5
3.	Information security investment is conveyed different stakeholders in a manner that is appropriate for their information technology security risk mitigation value.	1	2	3	4	5

2.12 considering future growth

Please rate level of agreement to the following statements. The number indicates the following statement.

Directions: (1- strongly Disagree 2- Disagree 3-Neutral 4-Agree 5- Strongly agree)

S.N	Factors	Choose				
1.	Your Organization does forecast the long and short-term growth goals before choosing a security solution.	1	2	3	4	5
2.	Your organization security investments are aligned with the organization mission.	1	2	3	4	5
3.	There is a proper information system security investment planning and execution of such a plan.	1	2	3	4	5

2.13 vendor involvement

Please rate/circle level of agreement to the following statements. The number indicates the following statement.

Directions: (1- strongly Disagree 2- Disagree 3-Neutral 4-Agree 5- Strongly agree)

S.N	Factors	Choose				
1.	There is an extreme vendor involvement in selections of security solutions.	1	2	3	4	5
2.	Vendor doesn't provides tools and assist in implementation of security solutions	1	2	3	4	5

3.	There is lack of transparent communication and participation with vendors in selections of security solutions.	1	2	3	4	5

2.14 Quality of information system security solutions

Please rate/circle level of agreement to the following statements. The number indicates the following statement.

Directions: (1- strongly Disagree 2- Disagree 3-Neutral 4-Agree 5- Strongly agree)

S.N	Factors	Choose				
1	The existing information system security solutions are easy to use.	1	2	3	4	5
2	The information system security solutions are flexible					
3	Your organization information system security solutions has a reliable functionality					

3.1 Information system security investment

Please rate/ circle your level of agreement with the following statements. The number indicates the following statement.

Directions: (1- strongly Disagree 2- Disagree 3-Neutral 4-Agree 5- Strongly agree)

S.N	Factors	Choose				
1.	Your organization's allocates resources on information system security preventive solutions.	1	2	3	4	5
2.	Your organization allocates resources on information system security detective measures					
3.	Your organization spend resources on information system security response measures					
4.	Your organization has an investment decision on non-technical measures					