COLLEGE OF BUSINESS AND ECONONMICS, SCHOOLOF COMMERCE

DEPARTMENT OF BUSINESS AND INFORMATION SYSTEMS

Information Security Governance Implementation Level in Ethiopian Banks

A Thesis By: Maereg Demeke, ID: GSR/9280/15

Advisor: Meshesha Legesse(Phd)

A Thesis submitted to the Department of Business Information Systems, College of Business and Economics, School of Commerce, Addis Ababa University, in partial fulfillment of the requirements of Master of Business Information Systems

September, 2024

Addis Ababa, Ethiopia

DECLARATION SHEET

The Student

I, the undersigned, declare that this thesis is my work and every material used has been duly acknowledged.

Name _____

Signature_____

Date of Submission_____

ADDIS ABABA UNIVERSITY

SCHOOL OF COMMERCE GRADUATE STUDIES

This is to certify that the thesis prepared by Maereg Demeke which is entitled "Information Security Governancae Implementation Level in Ethiopian Banks" submitted in partial fulfillment of the requirements for the Master of Arts in Business Information Systems complies with the regulations of the university and meets the accepted standards with respect to originality and quality.

Approved By Board of Examiners

Name of Advisor	Signature	Date
_____	_____	_____
Name of External Examiner	Signature	Date
_____	_____	_____
Name of Internal Examiner	Signature	Date
_____	_____	_____

ACKNOWLEDGMENTS

First of all, I would like to thank the Almighty God for giving me wisdom, strength, and courage to continue and finish my study. I would like to express my deepest gratitude to everyone who supported and contributed to the completion of this study. First and foremost, I am profoundly grateful to my advisor, Dr. Meshesha L., for his continuous guidance, encouragement, and invaluable insights throughout the research process. His expertise and unwavering support were instrumental in the successful completion of this work. Special thanks go to the banking professionals and institutions in Ethiopia who participated in this study. Their cooperation and willingness to share their experiences and insights were crucial for the data collection and analysis phases of this research. I am indebted to my colleagues and friends for their encouragement and constructive feedback. Their support kept me motivated and helped me refine my ideas. Finally, I would like to express my deepest appreciation to my family for their unconditional love, patience, and unwavering belief in me. Their constant support and encouragement have been my greatest source of strength throughout this journey. This study would not have been possible without the contributions and support of all these individuals and organizations. Thank you.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

ISG	Information Security Governance
COBIT	Control Objectives for Information and Related Technology
ISACA	Information Systems Audit and Control Association
ISO/IEC 27001	Information security, cybersecurity and privacy protection
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
ITIL	Information Technology Infrastructure Library

ABSTRACT

The main aim of this study was to assess the Information Security Governance Implementation Level in Ethiopian Banks. To this end, a descriptive survey research design has been employed taking 146 employees as samples to respond to the questionnaires designed for the study. The sampling method used was a stratified sampling method to select five banks(5) from a total of thirty-two (32) banks in Ethiopia. For the 146 respondents, a simple random sampling method was used. The data gathering instrument has been adopted from previous research which has made use of the COBIT (Control Objectives for Information and Related Technology) Framework which has five Governance objectives: Ensured Governance Framework, Ensured Benefit Delivery, Ensured Risk Optimization(EDM01), Ensured Resource Optimization(EDM02), and Ensured Stakeholders Engagement(EDM03). In this case, the study attempted to assess the existence of a relationship between each one of these objectives and with ISG Implementation level in Ethiopian Banks. Consequently, by using multiple regression analysis the study has found out that the variable with the highest beta value contributes the most explaining the dependent variable variance is EDM01 (0.333), followed by EDM04 (0.302), EDM02 (0.225), EDM05 (0.163), EDM03 (0.153). In general, all five objectives were found to have a statistically significant relationship towards ISG implementation level in which case the null hypotheses were rejected. Overall, the study found through descriptive analysis that the level of ISG implementation in Ethiopian banks is 3.78 which is 75.6%. The study has found different other findings according to the responses given by the respondents. The study has also made some recommendations to improve the ISG implementation level in Ethiopian banks.

Key Words: Information Systems Governance (ISG), COBIT Framework, Ensured Governance Framework, Ensured Benefit Delivery, Ensured Risk Optimization, Ensured Resource Optimization, Ensured Stakeholders Engagement.

CHAPTER ONE: INTRODUCTION

1.1. Background of the study

Information Security Governance (ISG) is defined as the set of responsibilities and practices exercised by the board and executive management to provide strategic direction, ensure that objectives are achieved, ascertain that risks are managed appropriately, and verify that the enterprise's resources are used responsibly (IT Governance Institute, 2006). It entails establishing an information security management framework that aligns with the organization's objectives, integrates with its risk management strategies, and ensures compliance with relevant laws and regulations (ISO/IEC 27014:2013). This framework is critical as it provides a structured approach to managing information security risks and aligns security efforts with business goals.

ISG also involves the development and implementation of policies, procedures, and guidelines designed to protect information assets from threats, ensuring their confidentiality, integrity, and availability. These elements are essential for creating a secure information environment and are typically based on international standards and best practices (Calder & Moir, 2008; Von Solms, 2008). Policies set the strategic direction for information security, procedures provide detailed steps for implementing policies, and guidelines offer recommendations to support the procedures. Together, these components help mitigate security risks, ensure compliance, and foster a culture of security within the organization.

Studies on the implementation of ISG have highlighted its critical role in safeguarding organizational assets and maintaining stakeholder trust. For instance, the IT Governance Institute (2006) emphasizes that effective ISG can help mitigate risks associated with information security breaches, ensuring that organizational operations are not disrupted. Calder and Moir (2008) argue that ISG enhances the ability of organizations to respond to security incidents and adapt to the evolving threat landscape. Moreover, Posthumus and Von Solms (2004) suggest that ISG plays a pivotal role in ensuring that information security initiatives are aligned with business objectives and that the necessary resources are allocated to manage information security risks effectively.

Research specific to the banking sector has demonstrated varied levels of ISG implementation across different regions. For example, a study by Al-Ahmad and Mohammad (2013) in the Middle East found that while banks are aware of the importance of ISG, there are significant gaps in its implementation, primarily due to inadequate executive support and

resource allocation. Similarly, Abu-Musa (2010) in Saudi Arabian banks highlighted the challenges faced in ISG implementation, including a lack of skilled personnel and insufficient integration with corporate governance practices. In a comparative study, Da Veiga and Eloff (2007) examined ISG implementation in South African banks and found that while regulatory requirements drive ISG efforts, there is still a need for a comprehensive approach that includes training and awareness programs to enhance the security culture within banks.

In the context of African banks, particularly in Ethiopia, there is limited research on the current state of ISG implementation. However, available studies suggest that the financial sector in Ethiopia is increasingly recognizing the need for robust information security practices. Mekonnen (2017) notes that Ethiopian banks have started to adopt information security frameworks, but the level of implementation varies significantly among institutions. Challenges such as limited technical expertise, financial constraints, and a lack of regulatory enforcement have been identified as key barriers to effective ISG implementation in the country (Mekonnen, 2017). Furthermore, a study by Bekele and Worku (2018) indicates that while there is a growing awareness of ISG among Ethiopian banks, the actual implementation of comprehensive ISG frameworks remains inconsistent, highlighting the need for a more structured approach to information security.

1.2. Statement of the Problem

In Ethiopia's financial sector, where digital payment systems and online banking services are rapidly evolving, information security governance is paramount to safeguarding customer financial information and maintaining trust in the banking system (Assefa et al., 2021).

The financial sector's shift towards digital solutions presents both opportunities and challenges, necessitating comprehensive strategies to safeguard against cyber threats and ensure the integrity of financial transactions (National Bank of Ethiopia, 2023). Studies carried out by cybersecurity companies continuously indicate a notable rise in cyberattacks globally on an annual basis. For instance, research by McAfee, 2021 shows a startling 125% increase in ransomware attacks from 2019 to 2020. Similarly, a report by IBM Security in 2022, reveals that the average cost of a data breach reached an all-time high of $4.35 million, with an increase of nearly 13% over the past two years, underscoring the growing financial impact of cyberattacks (IBM Security, 2022).

Ethiopia, characterized by a burgeoning economy and rapid digitization, has witnessed a significant expansion in its banking sector (Assefa & Abebe, 2019). This expansion has brought about an increased reliance on digital platforms for financial transactions, heightening the risk landscape for cyber threats (Dereje et al., 2021). Ethiopian banks, as integral components of the nation's financial infrastructure, are not immune to the challenges posed by cyber threats and vulnerabilities (Atnafu et al., 2020). Despite the growing recognition of the importance of ISG, the implementation level of ISG within Ethiopian banks remains a subject of concern(Dereje, Kidanemariam, & Bedasso, 2021). Furthermore, the consequences of inadequate ISG deployment go beyond cybersecurity, potentially weakening customer trust, harming business reputation, and resulting in financial losses (Yared & Solomon, 2020). In a highly competitive banking sector where trust and dependability are critical, fixing flaws in ISG implementation becomes critical to long-term economic survival.

Several studies have investigated cybersecurity challenges in the Ethiopian banking industry. For instance, Atnafu, Taddese, & Hailu (2020) discuss the broader cybersecurity challenges faced by the Ethiopian banking industry and propose countermeasures to address these challenges. It touches upon issues such as cyber threats, vulnerabilities, and potential strategies to enhance cybersecurity. Another study by Dereje, A., Kidanemariam, G., & Bedasso, M. (2021) introduces a maturity model for information security governance tailored to the banking industry in Ethiopia. It likely discusses the stages of maturity, key components, and factors contributing to the effective implementation of information security governance within Ethiopian private banks. A study by Solomon, S. (2018) explores the challenges and prospects of information security governance in the Ethiopian banking industry. It likely discusses factors hindering effective ISG implementation, potential solutions, and the overall outlook for enhancing cybersecurity governance within Ethiopian banks.

While existing literature provides valuable insights into cybersecurity challenges and theoretical frameworks for ISG, there is a notable gap in empirical research specifically focusing on the implementation level of ISG within Ethiopian banks.

This study aims to fill the gap in the existing literature by assessing the level of ISG implementation in Ethiopian banks, identifying the key challenges faced, and providing recommendations for enhancing information security practices in the sector. By doing so, it

seeks to contribute to the broader discourse on ISG and its critical role in maintaining the integrity and security of financial institutions. Through a comprehensive analysis of the current practices and challenges, this research will provide valuable insights for policymakers, banking executives, and information security professionals aiming to strengthen ISG in Ethiopian banks.

1.3. Research Questions

RQ1: what is the level of ISG implementation within Ethiopian banks?

RQ2: Is there a difference in the level of implementation of ISG in Ethiopian banks?

RQ3: what is the relationship between COBIT 2019 Governance Objectives and Information Security Governance Implementation Level in Ethiopian Banks?

RQ4: Which of the COBIT 2019 governance objectives has the highest implementation level?

1.4. Objectives of the Study

1.4.1 General Objective:

- To assess the level of information security governance (ISG) implementation in Ethiopian banks.

1.4.2 Specific Objectives:

- To determine whether there are significant differences in the level of information security governance implementation between Ethiopian banks.
- To investigate the relationship between the COBIT 2019 governance objectives and the overall information security governance implementation level in Ethiopian banks.
- To identify the COBIT 2019 governance objective with the highest level of implementation among Ethiopian banks.

1.5. Scope of the Study

The scope of this study is to investigate the level of information security governance implementation within Ethiopian banks. The study will focus specifically on assessing the level of information security governance implementation within the banking sector of Ethiopia. The research will involve data collection from a select number of banks operating in Ethiopia, utilizing quantitative research methods to gain insights into the current state of

information security governance within the sector. However, it will not delve into broader issues beyond the banking industry.

1.6. Definition of Terms

Information Systems Governance (ISG): Information Systems Governance refers to the processes, structures, and relational mechanisms in place to ensure that an organization's IT sustains and extends its strategies and objectives. It involves aligning IT strategy with business strategy, ensuring that investments in IT generate business value, and mitigating IT risks. ISG encompasses practices that ensure the effective, efficient, and acceptable use of IT within an organization (De Haes and Van Grembergen, 2004).

COBIT Framework: COBIT (Control Objectives for Information and Related Technology) is a framework created by ISACA for the governance and management of enterprise IT. COBIT provides a comprehensive set of practices, principles, models, and analytical tools to help organizations achieve their objectives for the governance and management of enterprise IT. It aligns IT with business goals and manages risks associated with IT (ISACA, 2012).

Ensured Governance Framework: An Ensured Governance Framework refers to a structured approach for governing IT that ensures IT activities are aligned with the business goals, and that resources are used responsibly. It includes policies, procedures, roles, and responsibilities designed to achieve strategic alignment, value delivery, risk management, resource management, and performance measurement (Weill and Ross, 2004).

Ensured Benefit Delivery: Ensured Benefit Delivery focuses on the realization of benefits from IT investments and initiatives. It involves ensuring that IT projects and services deliver the expected value and outcomes, aligning with the business objectives and providing measurable benefits (Ward and Daniel, 2012).

Ensured Risk Optimization: Ensured Risk Optimization is the process of identifying, assessing, and managing risks associated with IT in a manner that optimizes the risk-reward

balance. It involves implementing controls and strategies to mitigate potential negative impacts while maximizing the benefits of IT (ISACA, 2012).

Ensured Resource Optimization: Ensured Resource Optimization refers to the effective and efficient use of IT resources, including people, information, infrastructure, and applications, to meet the organization's objectives. It involves prioritizing and allocating resources in a way that maximizes value and supports the organization's strategy (IT Governance Institute, 2003).

Ensured Stakeholders Engagement: Ensured Stakeholders Engagement focuses on involving and aligning stakeholders, including business executives, IT professionals, and external partners, in the IT governance process. It aims to ensure that stakeholder needs and expectations are considered and addressed in IT decision-making and operations (Peterson, 2004).

1.8. Significance of the study

Practical significance: The practical significance of this study lies in its potential to provide valuable insights and recommendations for Ethiopian banks to enhance their information security governance practices. By evaluating the level of information security governance implementation and identifying key challenges, this research can assist banks in understanding their current security posture and areas for improvement. The findings can inform strategic decisions and investments in resources to strengthen information security measures, thereby mitigating cybersecurity risks and safeguarding sensitive data. Ultimately, the practical significance extends to improving the resilience of Ethiopian banks against cyber threats and enhancing trust and confidence among customers and stakeholders in the banking sector.

Theoretical Significance:- The theoretical significance of this study lies in its contribution to the academic discourse on information security governance, particularly within the context of emerging economies like Ethiopia. By examining the factors influencing the implementation of information security governance frameworks in Ethiopian banks, this research adds to the body of knowledge on the intersection of governance, cybersecurity, and organizational

practices. The findings can enrich existing theoretical frameworks and models in information security governance by providing empirical evidence and insights from a specific socio-economic context. Additionally, the study may stimulate further research in similar contexts or encourage comparative analyses across different industries or countries, thereby advancing the theoretical understanding of information security governance on a broader scale.

1.9. Organization of the Study

Chapter one is the introductory part which contains the background of the study, statement of the problem, basic research questions, objectives (general and specific objectives) of the study, significance of the study, delimitation and limitation of the study, and definition of terms. Chapter two will focus on a review of related literature to set the study within its wider context and to show the readers how the study supplements the work that has already been done on the topic. The research design, sample and sampling techniques, types and sources of data, data gathering instruments, the procedures of data collection, and method of data analysis will be included in chapter three, while data analysis will be presented in chapter four. Finally, findings, conclusions, and recommendations will be presented in chapter five.

1.10. Summary

In Chapter One, the study introduces the context of information security governance (ISG) within Ethiopian banks, highlighting the growing significance of ISG amidst escalating cyber threats in the digital era. The statement of the problem emphasizes the lack of comprehensive understanding regarding the effectiveness of ISG implementation in Ethiopian banks, prompting key research questions focusing on ISG effectiveness, influencing factors, primary challenges, and their impacts. The objectives of the study are outlined to assess current ISG implementation, identify influencing factors, explore challenges, and examine their impact on cybersecurity resilience. Additionally, the scope, definition of terms, and organization of the study are clarified to provide a structured framework for the research process.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

The literature review serves as the backbone of any research endeavor, offering a comprehensive examination of existing scholarly works, theories, and findings relevant to the research topic (Webster & Watson, 2002). It provides a solid foundation for understanding the current state of knowledge, identifying gaps, and shaping the research objectives and methodology. In the context of this study on information security governance (ISG) implementation in Ethiopian banks, the literature review consists of key concepts such as ISG frameworks, cybersecurity challenges in the banking sector, and best practices in ISG implementation.

2.2. Overview of the Ethiopian banking sector

Early Beginnings (19th Century)

The concept of banking in Ethiopia can be traced back to the 19th century, with the emergence of traditional money lenders and merchants engaging in primitive financial activities (National Bank of Ethiopia, 2020.). These informal arrangements served a limited purpose, primarily catering to a small segment of the population.

The Birth of Modern Banking (Early 20th Century)

The true foundation of Ethiopia's contemporary financial sector was established in the early twentieth century. The Bank of Abyssinia, the country's first chartered bank, was founded in 1906 using foreign money. This represented a substantial transition toward a more formal and regulated financial organization.

State Control and Consolidation (Mid-20th Century)

Following the 1974 Ethiopian Revolution, the government nationalized all private banks, ushering in a period of state dominance over the financial sector (Shiferaw et al., 2018). During this time, the emphasis moved to funding state-owned firms and promoting communist economic policy.

Opening Up and Diversification (Late 20th Century and Beyond)

The late twentieth century saw a substantial shift in Ethiopia's economic and political landscape. The government began liberalizing the banking sector after implementing market-oriented reforms. This prepared the path for the re-establishment of commercial banks and increased competition.

Ethiopia's quantity and diversity of financial institutions have increased since deregulation. Specialized banks catering to certain sectors, such as agriculture and manufacturing, have evolved alongside typical commercial banks. Furthermore, the establishment of microfinance banks has increased financial inclusion by reaching previously underserved parts of the population (Berhe & Jain, 2019).

The Digital Revolution

In recent years, Ethiopia's banking sector has embraced the digital revolution. The rapid growth of digital payment systems and online banking services is reshaping the way financial services are delivered (Asnake & Mulatu, 2022). While this digital leap offers numerous benefits, it also presents new information security challenges that Ethiopian banks need to address.

Ethiopia's banking sector changed dramatically in the late twentieth century as a result of economic liberalization. This age, highlighted by the reintroduction of private banks and increased competition, was also characterized by an increase in cyber attacks. As traditional brick-and-mortar businesses gave way to digital services such as online banking, the susceptibility of sensitive consumer data in electronic systems increased (Shiferaw et al., 2018). This underlines the critical need for strong information security measures to protect financial information and maintain trust in Ethiopia's expanding digital banking sector.

2.3. Regulatory Landscape of Information Security in Ethiopia

In Ethiopia, the regulatory landscape governing information security is shaped by various laws, regulations, and guidelines issued by regulatory authorities.

The National Bank of Ethiopia (NBE) Act mandates the NBE to regulate and supervise financial institutions, including banks, to ensure the stability and soundness of the financial system. Additionally, the NBE issues directives and guidelines on information security, data protection, and cybersecurity for banks to follow (National Bank of Ethiopia, 2020).

The Computer Crime Proclamation No. 958/2016 criminalizes various cyber offenses, such as unauthorized access to computer systems, data interference, and identity theft. This legislation aims to deter cybercriminal activities and protect critical information infrastructure in Ethiopia (Federal Negarit Gazeta, 2016).

Furthermore, the Personal Data Protection Proclamation No. 1243/2021 regulates the collection, processing, and storage of personal data by organizations, including banks, to safeguard individuals' privacy rights and prevent data breaches (Federal Negarit Gazeta, 2021).

Compliance with these regulatory requirements has a significant impact on information security governance in Ethiopian banks, influencing their policies, procedures, and risk management practices.

2.4 Motivation for ISG Implementation

To guarantee the privacy, availability, and integrity of organizational information assets, information security governance is essential (Weill & Ross, 2004; Whitman & Mattord, 2016). It encompasses the strategic management of policies, procedures, controls, and resources to protect information from unauthorized access, disclosure, alteration, or destruction. Effective information security governance aligns information security objectives with business goals, fosters a culture of security awareness, and enables organizations to adapt to evolving cybersecurity threats.

The importance of information security governance cannot be overstated, particularly in today's interconnected and data-driven business environment. As noted by Weill and Ross (2004), effective governance structures are essential for organizations to manage and mitigate cybersecurity risks while maximizing the value derived from their information assets. Information security governance provides a framework for decision-making, risk management, and resource allocation, helping organizations prioritize investments in cybersecurity measures based on their strategic objectives and risk tolerance levels. Table 2.1 shows a comparison between various ISG frameworks.

Table 2.1 Comparision of Most Used ISG Frameworks

Framework	Developer/Organization	Focus Areas	Key Features
COBIT	ISACA	IT governance, risk management, compliance	- Comprehensive set of control objectives and management guidelines
ISO/IEC 27001	ISO	Information security management, risk assessment, compliance	- Internationally recognized standard for information security management systems (ISMS)
NIST Cybersecurity Framework	NIST	Cybersecurity risk management, threat intelligence, incident response	- Framework for improving cybersecurity risk management in organizations
ITIL	Axelos	IT service management, service delivery, service support	Framework for managing IT services and aligning them with business needs

Source: (COBIT (ISACA, 2019); ISO/IEC 27001 (ISO/IEC, 2013); NIST Cybersecurity Framework (NIST, 2018); ITIL (Axelos, 2019))

To conduct this study, the COBIT 2019 framework has been chosen to assess the implementation level of ISG within Ethiopian banks. The decision to select COBIT 2019 is based on its well-established reputation for delivering business value through effective IT governance practices. As highlighted in previous discussions, COBIT is renowned for its comprehensive coverage of IT governance principles and its alignment with business objectives (ISACA, 2019). Specifically, COBIT's emphasis on linking IT processes to organizational goals makes it particularly relevant for the banking sector, where the delivery of services heavily relies on IT infrastructure and systems.

Developed by the IT Governance Institute (ITGI), COBIT provides a structured approach to IT governance, encompassing domains such as strategic alignment, value delivery, risk management, resource management, and performance measurement (ISACA, 2019). Its robust framework offers banks the necessary guidance and tools to ensure the alignment of IT investments and activities with business priorities. By leveraging COBIT, Ethiopian banks can effectively evaluate their ISG practices, identify areas for improvement, and enhance their overall cybersecurity posture (ISACA, 2019).

2.5. COBIT Framework

COBIT (Control Objectives for Information and Related Technology) is a widely recognized framework developed by ISACA (Information Systems Audit and Control Association) for the governance and management of enterprise IT. It provides a comprehensive set of controls and best practices to help organizations align their IT objectives with business goals, ensure effective risk management, and optimize IT resource utilization (ISACA, 2019).

COBIT defines a set of control objectives categorized into five domains: Evaluate, Direct, Monitor, Acquire, and Align (ISACA, 2019). These domains cover various aspects of IT governance, including By following the principles and guidelines outlined in COBIT, organizations can establish robust governance structures, implement effective controls, and achieve greater transparency and accountability in managing IT resources and risks.

Table 2.2 COBIT 2019 Framework Governance Objectives

Area	Domain	Objective ID	Objective	Objective Description	Objective Purpose Statement
Governance	Evaluate, Direct, and Monitor	EDM01	Ensured Governance Framework Setting and Maintenance	Analyze and articulate governance requirements for enterprise I&T, maintaining governance components.	Provide a consistent, aligned approach to governance, ensuring I&T decisions match enterprise strategy and compliance requirements.
Governance	Evaluate, Direct, and Monitor	EDM02	Ensured Benefits Delivery	Optimize value from business processes, I&T services, and assets.	Secure optimal value from I&T initiatives, ensuring cost-efficient solutions and accurate benefit projections.
Governance	Evaluate, Direct, and Monitor	EDM03	Ensured Risk Optimization	Understand and manage I&T-related risks within enterprise risk tolerance.	Ensure I&T risks are managed within enterprise tolerance, minimizing potential compliance failures.

Governance	Evaluate, Direct, and Monitor	EDM04	Ensured Resource Optimization	Ensure adequate I&T-related resources (people, process, technology) are available at optimal cost.	Optimize I&T resources and costs, enhancing benefit realization and future readiness.
Governance	Evaluate, Direct, and Monitor	EDM05	Ensured Stakeholder Engagement	Identify and engage stakeholders in I&T governance, ensuring transparent performance and conformance reporting.	Ensure stakeholders support I&T strategy, with effective communication and performance reporting aligned to enterprise strategy.

Source: ISACA (2019) COBIT 2019 Framework: Introduction and Methodology. Available at: https://www.isaca.org/resources/cobit (Accessed: 12 June 2024

2.6. Information Security Governance Focus Areas

Information Security Governance (ISG) is a critical aspect of organizational management that ensures the alignment of information security with business goals, effectively managing risks and resources, and delivering value. The following are the key focus areas of ISG:

Strategic Alignment

Strategic alignment refers to the harmonization of IT strategy with the overall business strategy to ensure that IT investments and initiatives support the achievement of organizational goals. Effective strategic alignment helps organizations leverage IT capabilities to drive business value and gain competitive advantages. In the context of information security, this means aligning security practices and policies with business objectives to protect critical assets while enabling business operations (ISACA, 2019).

Risk Management

Risk management in ISG involves identifying, assessing, and mitigating risks associated with information assets. It is a critical component for ensuring the confidentiality, integrity, and availability of information. An effective risk management framework helps organizations proactively address potential threats and vulnerabilities, thereby reducing the likelihood and impact of security incidents. This involves continuous risk assessment, risk treatment plans, and regular monitoring and review of risk management processes (ISO/IEC, 2018).

Resource Management

Resource management focuses on the efficient and effective deployment of IT resources, including personnel, infrastructure, and financial investments, to support the organization's information security goals. Proper resource management ensures that the organization has the necessary tools and skilled personnel to implement and maintain robust security measures. This area also encompasses capacity planning, budget management, and the allocation of resources to critical security initiatives (ISACA, 2019).

Performance Measurement

Performance measurement involves the use of key performance indicators (KPIs) and metrics to evaluate the effectiveness and efficiency of IT and information security processes. By

establishing and monitoring these metrics, organizations can assess their security posture, identify areas for improvement, and ensure that security initiatives are delivering the intended outcomes. Regular performance reviews and audits are essential to maintain high standards of information security (ISACA, 2019).

Value Delivery

Value delivery in ISG ensures that IT investments and security measures provide maximum value to the organization by supporting business objectives and enhancing operational efficiency. This involves optimizing IT services and resources to deliver tangible business benefits, such as improved productivity, reduced costs, and enhanced customer satisfaction. Effective value delivery requires a clear understanding of the organization's goals and the strategic use of IT to achieve these goals (IT Governance Institute, 2006).

2.7. Hypothesis Development

These hypotheses are developed based on the framework in Figure 2.3.

Table 2.3: Summary of the Hypotheses Formulated

Hypothesis
H01: There is no significant level of implementation of ISG in Ethiopian banks.
H02*:* There is no significant difference in the level of implementation of ISG in Ethiopian banks.
H03: There is no significant difference in the implementation levels of the different COBIT 2019 governance objectives in Ethiopian banks.
H04a: There is no significant relationship between the implementation level of ISG in Ethiopian banks and the COBIT 2019 governance objective Governance Framework (EDM01).

H04b: There is no significant relationship between the implementation level of ISG in Ethiopian banks and the COBIT 2019 governance objective Benefits Delivery (EDM02).

H04c: There is no significant relationship between the implementation level of ISG in Ethiopian banks and the COBIT 2019 governance objective Risk optimization (EDM03).

H04d: There is no significant relationship between the implementation level of ISG in Ethiopian banks and the COBIT 2019 governance objective Resource Optimization (EDM04).

H04e: There is no significant relationship between the implementation level of ISG in Ethiopian banks and the COBIT 2019 governance objective Stakeholders Engagement (EDM05).

2.8. The Proposed Framework

COBIT 2019 Governance Objectives as Independent Variables

The COBIT 2019 framework outlines a comprehensive set of governance and management objectives designed to ensure effective IT governance and management practices. These governance objectives serve as independent variables in this study.

ISG implementation level in Ethiopian banks as dependent variables

The implementation level of ISG in Ethiopian banks is the outcome or result of this study. It refers to the extent to which ISG practices, policies, and procedures are put into operation within these banks.

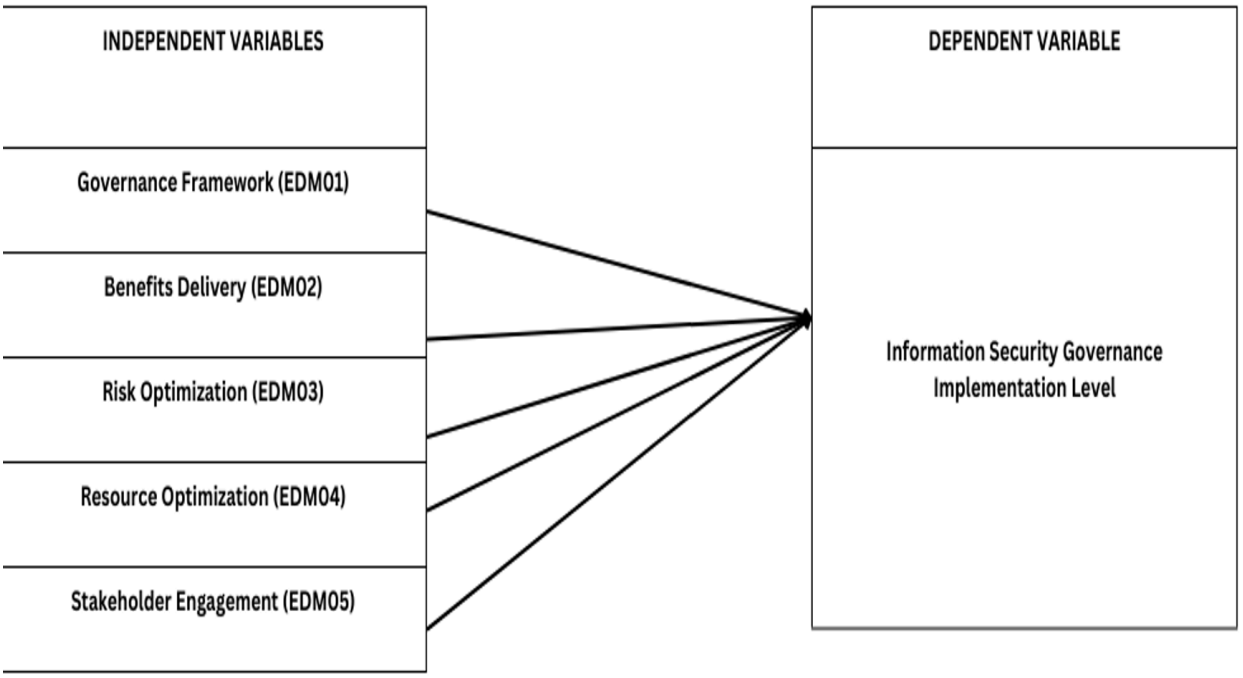


Figure 2.1 Proposed Framework of the Study

2.9. Summary

The literature review encompasses the importance of regulatory compliance and corporate governance in ensuring the stability and efficiency of financial institutions. Within this context, Information Systems Governance (ISG) emerges as a crucial component, serving as a framework for managing and controlling IT resources to align with organizational objectives. Various ISG models are discussed, with a notable emphasis on the COBIT (Control Objectives for Information and Related Technologies) framework, which offers guidelines and best practices for effective IT governance. The review underscores the significance of ISG in Ethiopian banks, emphasizing its role in enhancing operational efficiency, mitigating risks, and ensuring regulatory compliance within the dynamic banking environment of the region.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1. Introduction

This chapter outlines the approach that was applied to verify the study's hypothesis and meet the goals outlined in Chapter One. The theoretical foundation covered in chapter two was verified using the quantitative paradigm. Research design, developing hypotheses, population, sample, and statistical methods for data analysis are some topics covered in the debate.

3.3. Research Design and Method

The research objectives form the basis of the research design. The research used a descriptive research design to identify the information security governance implementation level in Ethiopian banks. This design was employed taking cross-sectional data that is going to be collected in one time shot. The study made use of quantitative data that is going to be collected from the employees of the selected banks.

3.4. Population of the Study

The population for this research comprises the banking industry in Ethiopia, totaling 32 banks.

Table 3.1 List of Banks in Ethiopia

Banks in Ethiopia		
Development Bank of Ethiopia	Abay Bank S.C.	Siket Bank S.C.
Commercial Bank of Ethiopia	Addis Int. Bank S.C.	Gedaa Bank S.C.
Awash Bank S.C.	Enat Bank S.C.	Amhara Bank S.C.
Dashen Bank S.C.	Global Bank S.C.	Tsehay Bank S.C.
Bank of Abyssinia	ZamZam Bank S.C.	
Wegagen Bank S.C	Shabelle Bank S.C.	

Hibret Bank S.C.	Goh Betoch Bank S.C.
Nib int. Bank S.C	Hijara Bank S.C.
Cooperative Bank of Oromia	Ahadu Bank S.C.
Lion International Bank	Sinqee Bank S.C.
Oromia Bank S.C.	Tsedey Bank S.C.
Zemen Bank S.C.	Omo Bank S.C
Bunna Bank S.C.	Sidama Bank S.C.
Berhan Bank S.C.	Rammis Bank S.C.

(*Source: https://nbe.gov.et/financial-institutions/banks/)*

3.5. Sampling

To facilitate sampling, these banks were categorized into five strata based on their high-profit achievement 2022/2023 fiscal year. After grouping the banks in five strata a random sampling method was used to select one bank from each strata.

3.6. Data Gathering Instrument

A structured five-point Likert scale was used to collect data. The survey consists of two parts, the biographic characteristics of respondents, and questions that involve the five governance objectives of the COBIT Framework. The instrument has been adapted from a previous similar study which has used this framework (Yaokumah, 2014).

The survey items were represented by a score on a 5-point Likert-type scale, where:

- 5 (fully implemented, FI) represents the maximum score of the scale;
- 4 (close to completion, CC);
- 3 (partially implemented, PI);
- 2 (planning stages, PS); and
- 1 (not implemented, NI) represents the minimum score.

3.7. Reliability and Validity

The validity of the instrument has been assessed by my Adviser as well as my colleagues. When it comes to reliability the instrument has been piloted in the study area taking a large sample considering those respondents who are not going to be involved in the main data collection. Once the data was collected in this way, the data has been encoded in the SPSS software for analysis.

3.8. Data Analysis Technique

The data to be collected has been analyzed in descriptive and inferential statistical methods. Concerning the descriptive analysis, the data collected were analyzed using mean scores and percentages. On the other hand, a correlation coefficient and multiple regression analysis were used to analyze the data with the intent of checking out the relationship between the independent variables and the dependent variable. A total of 275 questionnaires were distributed to employees, and only 146 completed questionnaires were found and encoded into the SPSS software once a sequential code was given to each questionnaire.

3.9. Ethical Considerations

This study abided by the ethical standards of research in the sense that all citations were duly acknowledged and listed in the reference section. All the citations and referencing followed the Harvard referencing style. The researcher secured a legal supporting letter from the department before asking for the consent of research participants in Ethiopian banks. In this regard, the researcher follows the legal and organizational structures to obtain the consent of the study company and its employees consequently. All the necessary explanations have been given to the research participants ahead of time.

3.10. Summary

Chapter Three presents a quantitative research methodology aimed at investigating the implementation level of Information Systems Governance (ISG) in Ethiopian banks, with COBIT 2019 framework objectives as Independent variables and the Implementation level of Information Systems Governance (ISG) as a dependent variable. The study formulated hypotheses to test this relationship, adhering to a sample size of five banks from a population of 32 Ethiopian banks. Data collection centered on a structured survey aligned with the

COBIT (Control Objectives for Information and Related Technologies) framework, allowing for a systematic analysis of ISG practices and implementation levels. Descriptive analysis techniques were applied to summarize survey responses, while multiple regression analysis was employed to explore the relationships between variables. Ethical considerations were paramount throughout the research process, ensuring participant confidentiality, informed consent, and avoidance of harm. Validity and reliability were addressed through pilot testing, expert review, and statistical analyses, ensuring the accuracy and consistency of findings in assessing ISG dynamics within Ethiopian banks.

CHAPTER FOUR: DATA PRESENTATION, INTERPRETATION AND DISCUSSION

4.1 Introduction

This chapter presents the discussions of the data analysis and findings obtained from the survey questionnaires. The first section is data cleaning, statistical assumptions; and factor analysis used to test the construct validity, internal consistency, and reliability analysis respectively. The findings from factor analysis, multiple regressions, and demographic characteristics are presented.

4.2 Response Rate

Table 4.1 presents the overall questionnaire sent and the response rate of the received questionnaire.

Table 4.1 Overall Response Rate

Response	Frequency	Response Rate
Overall Questionnaire distributed	275	
Uncompleted/wrongly filled questionnaire	38	
Usable Questionnarie	146	
Questionnaire returned	184	
Questionnaire not -returned	76	
Response rate'		66.9 %
Usable response rate		53.09 %

As the response rate was 53.09 %, it is considered to be adequate for data analysis. The data has been encoded into the SPSS computer software version 29. And the encoded data is then analyzed and presented hereunder and interpretations are made. Out of the total questionnaires distributed to 275 employees in the headquarters of the bank only 146 complete questionnaires were collected.

4.3 Data Cleaning

During the data cleaning, the researcher noticed some outrageous data through the descriptive analysis, and corrections were made before proceeding to further analysis. For data to be adequately prepared for statistical analysis, certain assumptions or guidelines must be adhered to. These include outliers among the cases, testing for normality, assessing multicollinearity, and ensuring homoscedasticity (Osborne & Waters, 2002).

4.3.1 Test for Outliers among Cases

Before conducting regression analysis, outlier should be identified if there are any. The total of cases deleted was thirty-eight (38), this reduced the number of respondents to one hundred and four six (146) in order to eradicate outliers totally. As shown in the picture below there are no circles or asterisks on either end of the box plot, this is an indication that no outliers are present after the data cleaning.

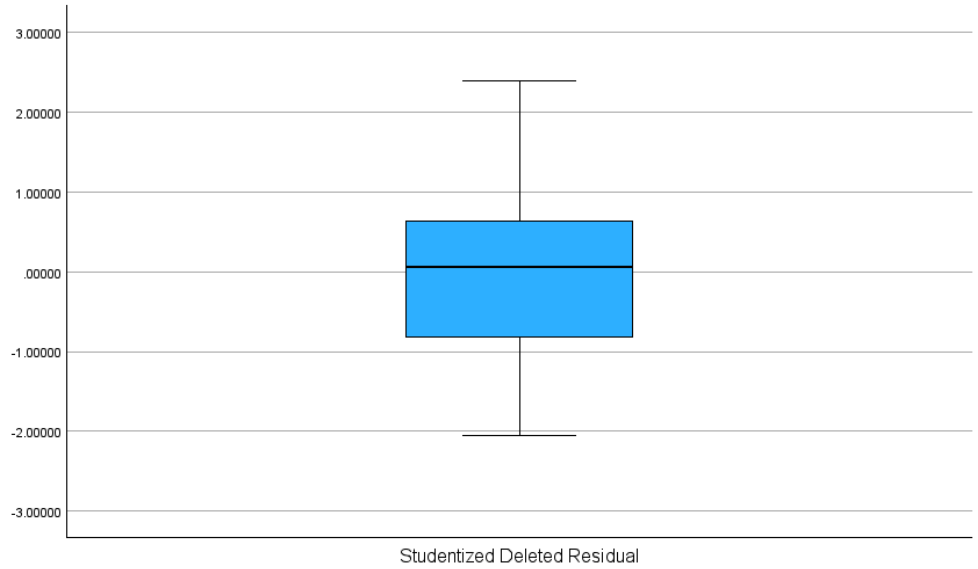


Figure 4.1: Result of test for outliers

4.3.2 Test of Normality

Table 4.2 Test of Normality

	Kolmogorov- Smirnova			Shapiro-Wilk		
	Statistic	df	Sig.	Static	df	Sig.
Studentized Residual	.056	131	.200*	.988	131	.292

The results obtained from the Shapiro-Wilk test indicate that all the variables had a p-value greater than(0.05), meaning that the variables involved in the Study follow a normal distribution: therefore, it can be concluded that the residual value is normally distributed so that regression analysis procedures have been fulfilled.

4.3.3 Homoscedasticity

Based on the scatterplot output, it appears that the spots are diffused and do not form a clear specific pattern, so it can be concluded that the regression model does not have a heteroskedasticity problem.

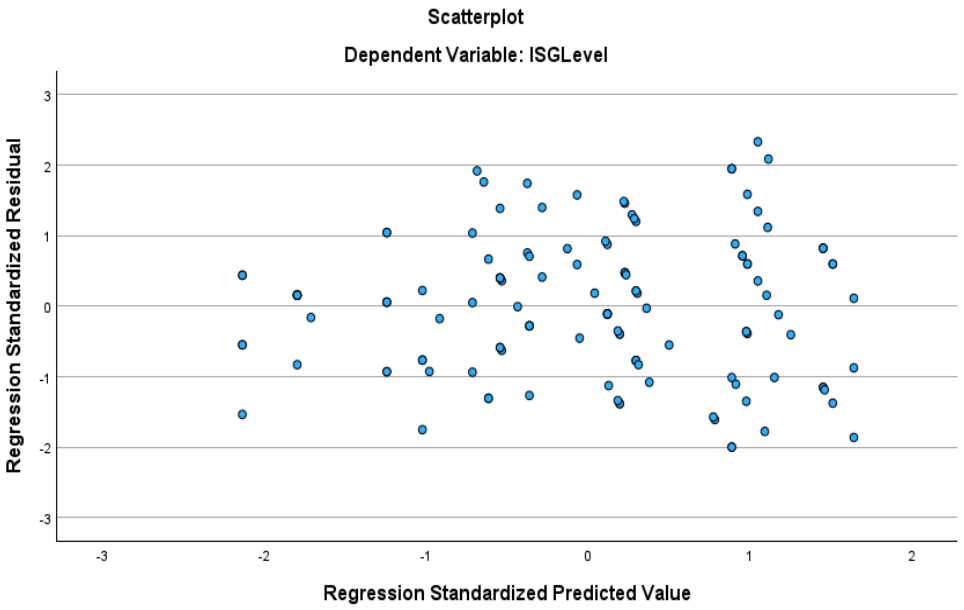


Figure 4.2 Scatter Plot Output

4.4 Demographic Representation of the Respondents

In this section, the demographic data collected from the employees is presented in the following table Table 4.3.

Table 4.3. *Demographic Representation of the Respondents*

Respondents	**Number of participants invited ()**	**The frequency of participants who responded (131)**	**(%)**
Position			
Board of Directors	5	2	0.4
Associate Cyber Security analyst	3	2	0.66
Chief Executive Officer	5	1	0.2
Chief Information Security Officer	5	4	0.8
Business or line managers	9	5	0.55
Cyber Security Director	7	3	0.42
Cyber Security Officer	13	4	0.3
Information Security Governance Officer	10	1	0.1
Information Security Governance and Risk officer	5	4	0.8
Information Security Officer	44	29	0.65
IT Audit Officer	15	11	0.73

IT Compliance Officer	13	4	0.3
IT Department	35	25	0.71
IT Director	16	10	0.62
IT Risk Analyst	22	7	0.31
IT Risk Officer	20	10	0.5
Human Resource Managers	6	2	0.33
IT Security Officer	23	12	0.52
Financial controllers or accountants	5	2	0.4
Other	14	8	0.57
Total	275	142	51.63
Duration			
<1 Year		8	
1-3 Years		82	
3-5 Years		30	
5-10 Years		20	
> 10 Years		6	
Total		146	

4.5 Reliability

Table 4.4 Reliability Test

No.	Objectives	Cronbach's Alpha	No. of items
1	EDMO1	.940	5
2	EDM02	.910	5
3	EDM03	.887	5
4	EDM04	.946	5
5	EDM05	.873	5

As we can observe from Table 4.4 all five objectives (EDM01 to EDM05) have Cronbach's Alpha values greater than 0.87, indicating high reliability. This means the items within each objective are consistently measuring their respective constructs.

4.5 Descriptive Analysis

RQ1: what is the level of information security governance (ISG) implementation within Ethiopian banks?

To answer this research question a descriptive analysis was performed on the data collected from the respondents addressing each of the five COBIT 2019 objectives. The result is stated as shown in the table below.

Table 4.5 Descriptive Statistics

		EDM01	EDM02	EDM03	EDM04	EDM05
N	Valid	131	131	131	131	131
	Missing	0	0	0	0	0
Mean		3.67	3.58	3.99	3.65	4.03
Std. Deviation		1.064	.914	.799	.963	.763

According to a study by Winfred Yaokumah's empirical study on information security governance implementation within Ghanaian industry sectors, the researcher mapped the

results as 1-not-implemented (20 percent), 2–planning stages (40percent), 3–partially implemented(60percent), 4–close to completion (80percent), and5–fully implemented (100percent). The average mean of the study results is **3.78** which lies down in the partially implemented to closed to completion stage.

RQ2: Is there a difference in the level of implementation of information security governance in Ethiopian banks?

Among the five strata(A, B, C, D, E) based on their high profit (A- very high capital, B- high capital, C- medium capital, D- medium-low Capital, and E- Low Capital) the following results were obtained by analyzing a comparison between the strata and ISG level implementation based on the mean value.

Table 4.6 Comparision among Ethiopian banks

Mean

Strata	**Avg. Mean**
A	4.19
B	4.45
C	4.17
D	4.00
E	2.97
Total	**3.78**

As shown by the table there is a significant difference in ISG Implementation level among Ethiopian banks. Hence hypothesis *H02:* There is no significant difference in the level of implementation of ISG in Ethiopian banks is rejected.

RQ3: Which of the COBIT 2019 governance objectives has the highest implementation level?

Based on the descriptive analysis results, the governance objective EDM05 - Ensure Stakeholders Engagement has the highest implementation level at 80.4%, indicating that it is

the most thoroughly implemented objective among the COBIT 2019 governance objectives within the organization.

H03: There is no significant difference in the implementation levels of the different COBIT 2019 governance objectives in Ethiopian banks is rejected.

4.5 Multiple Regression Analysis

Table 4.7 Analysis of variance result

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	74.933	5	14.987	365.242	<001[b]
	Residual	5.129	125	.041		
	Total	80.062	130			

a. Dependent Variable: ISG level

b. Predictors: (Constant), EDM05, EDM01, EDM03, EDM04, EDM02,

The ANOVA results indicate that the regression model is statistically significant ($F(5, 125) = 365.242$, $p < 0.001$), suggesting that the predictors explain a significant portion of the variance in the dependent variable.

4.5.1 Model Summary

Table 4.8 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin_watson
1	.967a	.936	.933	.20256	1.920

Predictors:(Constant), EDM01.EDM02, EDM03, EDM04, EDM05

Dependent Variable: ISG Implementation Level

From the description of the above table, 96.7% of the changes in the Information Security Implementation Level could be attributed to the combined effect of the predictor variables. However, 3.3% of the variance is explained by other factors not covered in this study.

4.5.2 Coefficients Table

RQ4: what is the relationship between COBIT 2019 Governance Objectives and Information Security Governance Implementation Level in Ethiopian Banks?

Table 4.9 Coefficients Table

Model		**Unstandardized B**	**Coefficients Std. Error**	**Standardized Coefficients Beta**	**t**	**Sig.**
1	Constant	-.029	.101		-290	.773
	EDM01	.245	.023	.333	10.702	<.001
	EDM02	.192	.037	.225	5.262	<.001
	EDM03	.150	.044	.153	3.399	<.001
	EDM04	.246	.033	.302	7.529	<.001
	EDM05	.167	.033	.163	5.140	<.001

Dependent Variable: ISG Implementation Level

Based on the coefficients table provided, we can assess the statistical significance and the contribution of each COBIT 5 objective (EDM01, EDM02, EDM03, EDM04, EDM05) to the dependent variable, ISG Level. The variable with the highest beta value contributes the most

explaining the dependent variable variance. EDM01(0.333), followed by EDM04(0.302), EDM02(0.225), EDM05(0.163), EDM03(0.153).
From the coefficients table:

- **EDM01**: t=10.702, p<.001
- **EDM02**: t=5.262, p<.001
- **EDM03**: t=3.399, p<.001
- **EDM04**: t=7.529, p<.001
- **EDM05**: t=5.140, p<.001

Since the p-values for all these variables are less than 0.05, we reject the null hypotheses for all COBIT 5 objectives. This indicates that each of these objectives has a significant effect on the ISG implementation level in Ethiopian banks. Hence,

H04a: There is no significant relationship between EDM01 and the level of Information Security Governance in Ethiopian banks. This null hypothesis was rejected.

H04b: There is no significant relationship between EDM02 and the level of Information Security Governance in Ethiopian banks. This null hypothesis was rejected.

H04c: There is no significant relationship between EDM03 and the level of Information Security Governance in Ethiopian banks. This null hypothesis was rejected.

H04d: There is no significant relationship between EDM04 and the level of Information Security Governance in Ethiopian banks. This null hypothesis was rejected.

H04e: There is no significant relationship between EDM05 and the level of Information Security Governance in Ethiopian banks. This null hypothesis was rejected.

4.5.3 Test for Multicollinearity

Table 4.10 : Collinearity

Model		Tolerance	VIF
1	Constant		

	EDM01	.530	1.886
	EDM02	.281	3.555
	EDM03	.254	3.937
	EDM04	.318	3.145
	EDM05	.512	1.953

Dependent Variable: ISG Implementation Level

All the VIF column values are less than 10, and Tolerance values are greater than 10% respectively, indicating that there is no multi-collinearity influence between the explanatory variables.

CHAPTER FIVE: SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Summary of Findings

The main purpose of this study was to asses the ISG implementation level in Ethiopian Banks. The study employed the COBIT 2019 Framework, focusing on five governance objectives: Ensured Governance Framework, Ensured Benefit Delivery, Ensured Risk Optimization, Ensured Resource Optimization, Ensured Stakeholdes Engagement. Specifically, the research aimed to assess implementation level and both the individual relationships between each governance objectives and ISG implementation, as well as the aggregate relationship of all five governance dimensions.

The research questions addressed were:
What is the level of ISG implementation within Ethiopian banks?
Is there a difference in the level of implementation of ISG in Ethiopian banks?
What is the relationship between COBIT 2019 Governance Objectives and Information Security Governance Implementation Level in Ethiopian Banks?
Which of the COBIT 2019 governance objectives has the highest implementation level?

A total of 275 questionnaires were distributed to employees, with 146 completed questionnaires returned. The data was analyzed using SPSS software, leading to the following major findings:

- The level of of ISG implentation was found to be m= 3.78 (75.6%)
- There is a difference in implement ISG Ethiopian banks.
- A statistically significant relationship was found between the Governance Objectives and ISG implementation in Ethiopian Banks.
- EDM05 (Ensured Stakeholdes Engagement) was found to be the one with highest implementation level.

5.2 Limitations

- The reliance on self-reported data through surveys or assessments may introduce bias, as respondents might overestimate the implementation levels of governance objectives.
- The cross-sectional nature of the study provides a snapshot at a single point in time, limiting the ability to observe changes or trends in governance objective implementation over time.

5.3 Conclusions

Based on the findings of the study, the following conclusions have been made, the study aimed to assess the level of Information Security Governance (ISG) implementation in Ethiopian banks and to explore the relationship between COBIT 2019 governance objectives and ISG implementation. Based on the findings, several key conclusions can be drawn:

Level of ISG Implementation:

The ISG implementation in Ethiopian banks was found to be partially implemented, with an average score of 3.78, which translates to 75.6 %. This indicates that while there are efforts towards implementing ISG practices, there is still room for improvement to achieve full implementation.

Variability in ISG Implementation:

There is a notable difference in the level of ISG implementation across different Ethiopian banks. This suggests that some banks may have more advanced ISG practices compared to others, highlighting the need for a more uniform approach to ISG across the sector.

Relationship Between Governance Objectives and ISG Implementation:

A statistically significant relationship was identified between the COBIT 2019 governance objectives and the level of ISG implementation in Ethiopian banks. This signifies that effective implementation of these governance objectives is crucial for enhancing ISG practices.

Highest Implemented Governance Objective:

Among the COBIT 2019 governance objectives, EDM05 - Ensure Stakeholders Engagement was found to have the highest implementation level. This indicates that Ethiopian banks place significant emphasis on engaging stakeholders in their governance processes. Stakeholder engagement is essential for ISG as it ensures that the interests and concerns of all relevant parties are considered, leading to more comprehensive and effective security measures.

5.4 Recommendations

Focus on Comprehensive ISG Implementation: Banks need to strive towards fully implementing ISG practices beyond the current partial implementation. This can involve enhancing policies, procedures, and technologies related to information security.

Addressing Disparities in ISG Implementation: To address the variability in ISG implementation, regulatory bodies and bank management should work towards establishing standardized ISG frameworks and best practices that can be uniformly adopted across all banks.

Enhancing Governance Objectives: Given the significant relationship between governance objectives and ISG implementation, banks should focus on strengthening all COBIT 2019 governance objectives. This includes ensuring that objectives such as risk optimization, resource management, and benefit realization are also effectively implemented alongside stakeholder engagement.

Promoting Stakeholder Engagement: The high implementation level of EDM05 suggests that banks should continue to prioritize stakeholder engagement. This can be further enhanced by regular communication, feedback mechanisms, and inclusive decision-making processes involving all stakeholders.

5.4 Recommendations for Future Research

Future studies could expand the scope to include more banks and possibly compare ISG implementation across different sectors within Ethiopia or other countries. Conducting longitudinal studies to observe changes and improvements in ISG implementation over time

would provide deeper insights into the effectiveness of various initiatives.Further research could analyze the specific impacts of different governance objectives on ISG outcomes to identify which areas yield the most significant improvements in security governance.

REFERENCES

IT Governance Institute (2006) Information Security Governance: Guidance for Boards of Directors and Executive Management. 2nd edn. Illinois: IT Governance Institute.

ISO/IEC 27014:2013 (2013) Information technology — Security techniques — Governance of information security. Geneva: International Organization for Standardization.

Calder, A. and Moir, S. (2008) IT Governance: Implementing Frameworks and Standards for the Corporate Governance of IT. 4th edn. London: IT Governance Publishing.

Von Solms, B. and Von Solms, R. (2008) *Information Security Governance*. New York: Springer.

Al-Ahmad, W. and Mohammad, B. (2013) 'Addressing Information Security Risks by Adopting Standards', International Journal of Information Management, 33(5), pp. 725-728.

Abu-Musa, A.A. (2010) 'Exploring Information Security Governance in Saudi Arabian Banks: An Empirical Study', Information Management & Computer Security, 18(4), pp. 226-276.

De Haes, S. and Van Grembergen, W. (2004) 'IT governance and its mechanisms', Information Systems Control Journal, 1, pp. 27-33.

Mekonnen, G. (2017) 'Information Security Management in Ethiopian Banking Sector', Journal of Information Security and Applications, 34, pp. 67-75.

Bekele, R. and Worku, G. (2018) 'Information Security Practices in Ethiopian Banking Industry', *International Journal of Information Security Science*, 7(2), pp. 12-19.

Assefa, B., Shimelis, A., & Minten, B. (2021). Maturity of information systems' security in Ethiopian banks: the case of selected private banks.

National Bank of Ethiopia, 2023. Annual Report 2023. [online] Available at: https://www.nbe.gov.et/report/annual2023.pdf [Accessed 12 June 2024].

McAfee, 2021. New McAfee Report Reveals Alarming Rise in Ransomware Attacks, Highlighting the Need for Proactive Defense. Accenture. [online] Available at: https://newsroom.accenture.com/news/new-mcafee-report-reveals-alarming-rise-in-ransomware-attacks-highlighting-the-need-for-proactive-defense.htm [Accessed 12 June 2024].

IBM Security, 2022. Cost of a Data Breach Report 2022. [online] Available at: https://www.ibm.com/security/data-breach [Accessed 12 June 2024].

Assefa, A. A., & Abebe, L. A. (2019). Challenges of E-banking services: Ethiopian perspective. International Journal of Scientific & Technology Research, 8(12), 1437-1443.

Dereje, A., Kidanemariam, G., & Bedasso, M. (2021). Information security governance maturity model for the banking industry in Ethiopia. Journal of Information Security, 12(1), 10-25

Yared, T. M., & Solomon, A. T. (2020). The impact of information security governance on bank performance in Ethiopia: The mediating role of information security culture. Journal of Information Security, 11(3), 78-90.

Atnafu, D. G., Taddese, H., & Hailu, G. G. (2020). Cybersecurity challenges and countermeasures in the Ethiopian banking industry. In Proceedings of the 2020 6th International Conference on Information Management (ICIM) (pp. 68-72).

Solomon, S. (2018). Challenges and prospects of information security governance: The case of Ethiopian banking industry. Journal of Information Security, 9(3), 127-139.

ISACA (2012) COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. ISACA.

Weill, P. and Ross, J.W. (2004) IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. Harvard Business School Press.

Ward, J. and Daniel, E. (2012) Benefits Management: How to increase the business value of your IT projects. John Wiley & Sons.

IT Governance Institute (2003) Board Briefing on IT Governance, 2nd edn. IT Governance Institute.

Peterson, R. (2004) 'Integration Strategies and Tactics for Information Technology Governance', in Van Grembergen, W. (ed.) Strategies for Information Technology Governance. Idea Group Publishing, pp. 37-80.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. MIS quarterly, 26(2), xiii-xxiii.

National Bank of Ethiopia. (2020). Banking Business Directives. Retrieved from https://www.nbe.gov.et/banking-business-directives

Shiferaw, B., Merkebu, A., & Mitiku, A. (2018). Bank Information Systems Vulnerability: The Case of Ethiopia.

Berhe, Y., & Jain, S. (2019, January). AIS Electronic Library (AISeL) - AMCIS 2019 Proceedings: Factors Hindering Full-Fledged Information Security in the Banking Sector in Ethiopia.

Federal Negarit Gazeta. (2016). Computer Crime Proclamation No. 958/2016. Retrieved from http://www.natlex.org/natlex4/detail.htm?id=36098

Federal Negarit Gazeta. (2021). Personal Data Protection Proclamation No. 1243/2021. Retrieved from http://www.natlex.org/natlex4/detail.htm?id=36423

ISACA. (2019). COBIT 2019 Framework: Introduction and Methodology. Information Systems Audit and Control Association.

Osborne, J. W., & Waters, E. (2002). Four assumptions of multiple regression that researchers should always test. Practical Assessment, Research, and Evaluation, 8(1), 2.

ISO/IEC 27000:2018. (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary. International Organization for Standardization.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology.

APPENDICES

Appendix 1: Questionnaire

ADDIS ABABA UNIVERSITY

College of Business and Economics School of Commerce

Department of Business Information System

MA Program in Business Information Systems

Introduction

Dear Participant,

Thank you for taking the time to participate in this survey. This study aims to evaluate the implementation of Information Security Governance (ISG) within Ethiopian banks by using the COBIT 2019 framework (Control Objectives for Information Technologies). By assessing the current practices and frameworks in place, we aim to identify strengths, weaknesses, and areas for improvement. Your valuable input will significantly enhance Information Security Governance practices, ensuring that our financial institutions are better protected against information security threats.

We understand the importance of confidentiality and assure you that your responses will be confidential. All data collected will be used solely for research purposes and reported in aggregate form, ensuring no individual respondent can be identified. A copy of the paper produced may be provided to you if so demanded. Your honest responses are crucial for the success of this study, and we appreciate your cooperation.

Thank you once again for your participation.

Sincerely,

Maereg Demeke
MBIS Graduate Student

School of Commerce, Addis Ababa University
maeregdemeke01@gmail.com

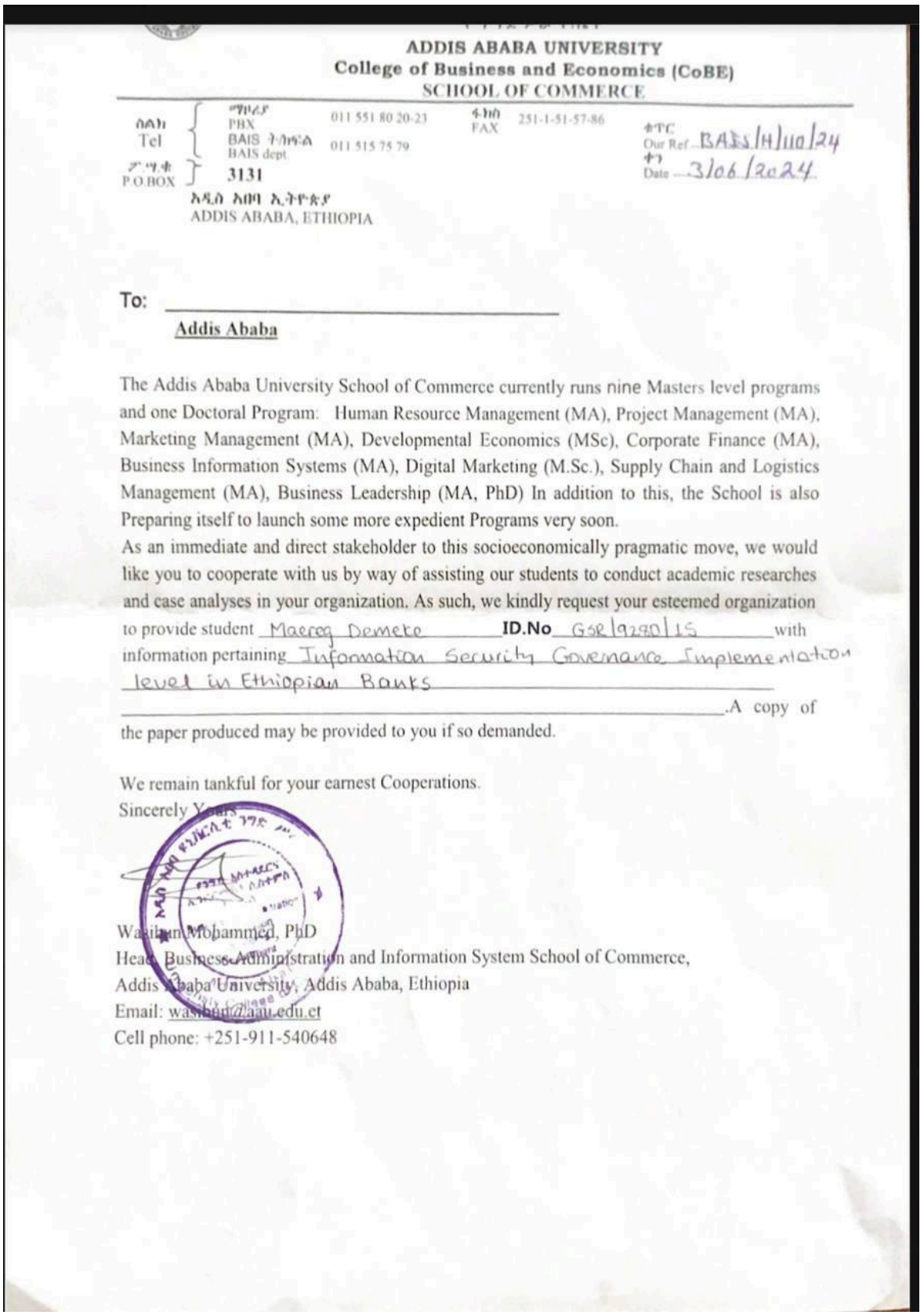
Note: • 5 (fully implemented, FI) represents the maximum score on the scale; • 4 (close to completion, CC); • 3 (partially implemented, PI); • 2 (planning stages, PS); and • 1 (not implemented, NI) represents the minimum score.

#	Question	NI	PS	PI	CC	FI
Governance Framework (EDM01)						
1	To what extent is our bank's governance framework for managing information security well-established?					
2	How regularly is the governance framework reviewed and updated to address new security challenges?					
3	How clearly are roles and responsibilities for information security defined within our bank?					
4	To what extent does the governance framework align with the bank's overall business strategy?					
5	How comprehensive are the specific policies for information security included in the governance framework?					
Benefits Delivery (EDM02)						
6	To what extent does our bank optimize the value from investments in business processes, IT services, and IT assets?					
7	How thoroughly are IT investments evaluated to ensure they deliver expected benefits to the business?					
8	How regularly does the bank assess whether IT investments are aligned with business goals?					
9	To what extent are business process improvements tracked to measure their impact on organizational performance?					
10	How clear is the process for identifying and capitalizing on IT-related opportunities?					

Risk Optimization (EDM03)						
11	How comprehensive is our bank's process for identifying information security risks?					
12	How regularly are information security risks assessed and prioritized?					
13	To what extent are appropriate measures in place to mitigate identified risks?					
14	How are the bank's risk appetite and tolerance defined and communicated?					
15	To what extent are risk management practices integrated with overall business risk management?					
Resource Optimization (EDM04)						
16	How sufficient are the resources (financial, human, technological) allocated for information security initiatives?					
17	How well are information security investments aligned with our bank's strategic objectives?					
18	How thorough is the process for evaluating the return on investment for information security expenditures?					
19	To what extent are resources for information security utilized efficiently?					
20	How regularly does the bank review and adjust resource allocation for information security?					
Stakeholder Engagement (EDM05)						
21	How are information security policies and procedures communicated to all employees?					
22	How regularly is information security activity reported to senior management and the board of directors?					

23	To what extent are stakeholders involved in the decision-making process regarding information security?					
24	How transparently are information security incidents and responses communicated to relevant stakeholders?					
25	How well does the bank ensure accountability and transparency in all information security practices?					
Information Security Governance Implementation Level						
26	To what extent has your bank integrated its IT strategy with its business strategy?					
27	How well has your bank implemented a formal risk management framework to identify, assess, and mitigate IT-related risks?					
28	To what extent has your bank effectively allocated and managed IT resources (e.g., personnel, infrastructure) to meet its strategic objectives?					
29	How thoroughly has your bank established and utilized key performance indicators (KPIs) to measure the effectiveness of its IT processes?					
30	How effectively has your bank optimized its IT investments to ensure they deliver maximum value and align with business goals?					

Appendix 2: Letter of recommendation



ADDIS ABABA UNIVERSITY
College of Business and Economics (CoBE)
SCHOOL OF COMMERCE

ስልክ Tel: ማዕከል PBX 011 551 80 20-23; BAIS ትምህርት BAIS dept 011 515 75 79; ፋክስ FAX 251-1-51-57-86
ፖ.ሣ.ቁ P.O.BOX 3131
አዲስ አበባ ኢትዮጵያ
ADDIS ABABA, ETHIOPIA

ቁጥር Our Ref. BAIS/H/110/24
ቀን Date 3/06/2024

To: _____
Addis Ababa

The Addis Ababa University School of Commerce currently runs nine Masters level programs and one Doctoral Program: Human Resource Management (MA), Project Management (MA), Marketing Management (MA), Developmental Economics (MSc), Corporate Finance (MA), Business Information Systems (MA), Digital Marketing (M.Sc.), Supply Chain and Logistics Management (MA), Business Leadership (MA, PhD) In addition to this, the School is also Preparing itself to launch some more expedient Programs very soon.

As an immediate and direct stakeholder to this socioeconomically pragmatic move, we would like you to cooperate with us by way of assisting our students to conduct academic researches and case analyses in your organization. As such, we kindly request your esteemed organization to provide student Maereg Demeke ID.No GSR/9280/15 with information pertaining Information Security Governance Implementation level in Ethiopian Banks _____.A copy of the paper produced may be provided to you if so demanded.

We remain tankful for your earnest Cooperations.

Sincerely Yours

Wasihun Mohammed, PhD
Head, Business Administration and Information System School of Commerce,
Addis Ababa University, Addis Ababa, Ethiopia
Email: wasihun@aau.edu.et
Cell phone: +251-911-540648