ADDIS ABABA UNIVERSITY

COLLEGE OF BUSINESS AND ECONOMICS

DEPARTMENT OF ACCOUNTING AND FINANCE

ASSESSMENT ON THE SECURITY OF ACCOUNTING INFORMATION SYSTEM IN THE BANKING SECTOR IN ETHIOPIA: THE CASE OF ZEMEN BANK

BY:

ETSUBDINK ENDALE

JUNE, 2024.

ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

COLLEGE OF BUSINESS AND ECONOMICS

DEPARTMENT OF ACCOUNTING AND AUDITING

ASSESSMENT ON THE SECURITY OF ACCOUNTING INFORMATION SYSTEM IN THE BANKING SECTOR IN ETHIOPIA: THE CASE OF ZEMEN BANK

A PROJECT SUBMITTED TO THE DEPARTMENT OF ACCOUNTING AND FINANCE IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN ACCOUNTING AND AUDITING

BY:

ETSUBDINK ENDALE

ADVISOR:

HABTAMU BERHANU (PHD)

JUNE, 2024.

ADDIS ABABA, ETHIOPIA

Declaration

I, Etsubdink Endale declare that this paper is a result of my independent research work on the topic entitled "ASSESSMENT ON THE SECURITY OF ACCOUNTING INFORMATION SYSTEM in the banking sector in Ethiopia: The case of Zemen bank" in partial fulfillment of the requirements for the Degree of Masters of Science in Accounting and Auditing at Addis Ababa University. This work has not been submitted for a degree to any other university. All the references are also duly acknowledged.

Etsubdink Endale

Signature 

Date July-03-2024

Confirmation

This is to certify that Etsubdink Endale has carried out this research work on the topic entitled "Analysis on the factor affecting security of accounting information system in the banking sector in Ethiopia: The case of Zemen bank" under my supervision. This work is original in nature and has not been presented for a degree in any University and it can be submitted for the partial fulfillment of the requirements for the award of the degree of Masters of Science Accounting Finance.

DR. Habtamu Berhanu

Signature_ 

Date _July-03-2024

ADDIS ABABA UNIVERSITY

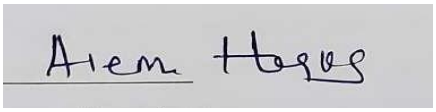
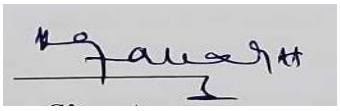
COLLEGE OF BUSINESS AND ECONOMICS

ASSESSMENT ON THE SECURITY OF ACCOUNTING INFORMATION SYSTEMIN THE BANKING SECTOR IN ETHIOPIA: THE CASE OF ZEMEN BANK

BY:

ETSUBDINK ENDALE

Approved by a board of Examiners and Advisor:

Habtamu Birhanu (Dr.)		**July-03-2024**
Advisor	**Signature**	**Date**
		**July-03-2024**
Examiner	**Signature**	**Date**

Acknowledgement

I would like to express my profound gratitude to the divine guidance of God and the intercessions of his mother, St. Mary, who have been my constant source of strength, hope, and inspiration throughout my life's journey. Their boundless grace, protection, and wisdom have been pivotal in shaping my endeavors and illuminating the path to achievement.

I extend my deepest appreciation to my esteemed advisor, Dr. Habtamu, whose scholarly wisdom, mentorship, and insightful guidance have been instrumental in shaping the depth, rigor, and academic integrity of this research. His expertise, support, and encouragement have played a pivotal role in nurturing my intellectual growth and shaping the trajectory of this scholarly endeavor.

I am profoundly thankful to my dedicated assistant, Tsegaye Agede, whose unwavering commitment, collaboration, and indispensable contributions have significantly enriched this research endeavor. His diligent efforts have been pivotal in facilitating the execution and completion of various components, underscoring the collaborative spirit that has propelled this work forward. Furthermore, I express my heartfelt gratitude to my beloved mother, Sehen, for her unwavering love, guidance, and selfless support at every stage of my life's journey, including this research project. Her unwavering strength, encouragement, and nurturing spirit have been a constant source of inspiration, providing the foundation for my personal and academic growth.

Lastly, I extend my sincere appreciation to all the staff of Zemen Bank for their invaluable assistance and cooperation, which significantly enriched the depth and quality of this research. Their willingness to share insights, resources, and support has been instrumental in shedding light on the intricate dynamics of financial inclusion and economic development within the banking domain.

List of Acronyms

AIS	Accounting Information System
AICC	Accounting Information Communication Control
ACFE	Association of Certified Fraud Examiners
COBIT	Control Objectives for Information and Related Technology
COSO	Commute of sponsoring organization
ETA	Employee Training and Awareness
IFRS	International Financial Reporting Standards
PCI DSS	Payment Card Industry Data Security Standards
SAIS	Security of Accounting Information system
SOX	Sarbanes-Oxley Act
SPSS	Statistical Package for the Social Sciences
TOGAF	The Open Group Architecture Framework
UA	User Authentication
ZB	Zemen Bank

Contents

List of Table

List of figures

Abstract

The paper delves into the critical issue of accounting information system (AIS) security within the Ethiopian banking sector, with a specific focus on Zemen bank. The study aims to comprehensively understand the factors influencing the security of AIS in this context. The dependent variable, security of AIS, is influenced by several independent variables, including security measures and control, user authentication methods, employee training and awareness, and technology infrastructure within Zemen bank's AIS. The research seeks to investigate the challenges and vulnerabilities associated with security measures and control within Zemen bank's AIS. It aims to understand the effectiveness of existing security protocols and identify potential weaknesses that may compromise the security of the system. Additionally, the study analyze user authentication methods to determine their impact on AIS security, as well as evaluate employee training and awareness programs to gauge their effectiveness in mitigating security risks. Furthermore, the research will delve into the technological infrastructure supporting Zemen bank's AIS to assess its role in ensuring the security of financial information. By examining these independent variables, the study aims to provide insights that can guide the development of effective strategies and policies to enhance the security of AIS in Ethiopian banks, ultimately contributing to the protection of sensitive financial information and the overall resilience of the banking sector. In conclusion, this research paper aims to contribute to the understanding of AIS security in the Ethiopian banking sector, with a specific focus on Zemen bank. By examining the factors influencing AIS security, including security measures and control, user authentication methods, employee training and awareness, and technology infrastructure, the study seeks to provide valuable insights that can inform the development of robust security strategies and policies. Ultimately, the findings of this research are expected to contribute to the protection of sensitive financial information and bolster the overall resilience of the banking sector in Ethiopia.

***Key words**: Accounting Information System, Cybersecurity, Technology Infrastructure, Access Controls, Employee Training*

CHAPTER ONE

INTRODUCTION

1.1. Background of the study

An accounting information system (AIS) is a system that collects, stores, and processes data and provides information to users about the financial activities and status of an organization and also processes data about the financial transactions of an organization and provides information to users for decision-making. (Laudon & Laudon, 2020)

The AIS is responsible for providing the information that decision-makers need to make sound financial decisions. It does this by collecting data from transactions, processing that data into meaningful information, and storing that information in a way that it can be easily retrieved. The AIS also reports the information to decision-makers in a way that is easy to understand and use. The AIS is an essential part of any organization. It provides the information that is needed to track financial performance, manage resources, and make strategic decisions. Without effective AIS, organizations would be unable to make informed decisions about their financial future. (Hansen & Mowen, 2021)

The AIS plays a crucial role in various business processes, including financial reporting, management reporting and cost accounting. The key components of the AIS include hardware, software, people, procedures, and data. AIS must adhere to the five basic principles of accounting: relevance, reliability, comparability, consistency, and understandability. It should also comply with regulatory requirements, industry standards, and organizational policies and procedures. (Hall, 2017)

AIS are essential for banks to operate effectively. They provide the information that bank managers need to make sound financial decisions, and they help banks to track customer accounts and manage risk. AIS also play a role in compliance with regulations, such as those governing anti-money laundering and Know Your Customer (KYC). The evolution of AIS in banks has been driven by a number of factors, including the increasing complexity of financial transactions, the growth of electronic banking, and the need to comply with new regulations. Early AIS were mainframe-based systems that were designed to track and record financial transactions. These systems were often slow and inefficient, and they were not able to keep up with the pace of change

in the banking industry. In recent years, there has been a shift towards client-server and web-based AIS. These systems are more flexible and scalable, and they can be accessed from anywhere in the world. They also have the ability to integrate with other systems, such as customer relationship management (CRM) and fraud detection systems. (Wang & Shen, 2016).

Information security is the protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure its confidentiality, integrity, and availability. (Whitman & Mattord 2017)

1.2. Statement of the problem

Assessment on the security of accounting information system in banking sector in Ethiopia in banks is a complex and challenging task. Banks are increasingly reliant on AISs to process financial transactions, and the security of these systems is essential to protect customer data and prevent fraud. However, banks are also targets for cyberattacks, and the security of their AISs is constantly under threat. (Al-Hujran & Weerakkody, 2018)

Accounting information systems (AIS) are essential for the efficient and effective operation of businesses. However, AIS are also vulnerable to security threats, such as unauthorized access, data manipulation, and system disruptions. These threats can have a significant impact on a business, including financial losses, reputational damage, and regulatory penalties. Auditors play an important role in ensuring the security of AIS. They can assess the effectiveness of an organization's security controls and identify areas where improvements are needed. However, there is a lack of research on the specific auditing techniques that are most effective for AIS security. (Janvrin, et al, 2009)

The paper assessment on the security of AIS is important for a number of reasons. First, it can help to identify and mitigate security risks to AIS. Second, it can help to ensure that AIS are compliant with relevant regulations. Third, it can help to improve the overall security posture of businesses. (Janvrin, et al, 2017)

Another challenge is the increasing use of technology in business. Technology can make it easier for businesses to process transactions and record data. However, it can also make it easier for businesses to commit fraud or manipulate financial information. (Mautz, 1984)

The paper aims to address the critical issue of accounting information system (AIS) security within the banking sector of Ethiopia, with a specific focus on Zemen bank. The problem revolves around the need to comprehensively understand the factors influencing the security of AIS in this context. The study seeks to investigate the challenges and vulnerabilities associated with security measures and control, user authentication methods, employee training and awareness, and technology infrastructure within Zemen bank's AIS. By identifying and analyzing these factors, the research aims to provide insights that can guide the development of effective strategies and policies to enhance the security of AIS in Ethiopian banks, ultimately contributing to the protection of sensitive financial information and the overall resilience of the banking sector.

In conclusion, the study provides valuable insights into the current security measures in place and identify any gaps or weaknesses. The findings of the study helps the bank to improve the security of its AIS and protect its customers' data.

1.3. Research Questions

To answer the problem statement, the following broad and specific research questions are proposed

1. What are the potential vulnerabilities and threats that could compromise the security of AIS at Zemen Bank?
2. How effective are the existing security controls, their implementation procedures and the measures in mitigating risk with in the AIS of Zemen Bank?
3. What are the future trends and emerging technologies that can enhance the security of the AIS at Zemen Bank?

1.4. Research Objectives

The objective of the study consists of general and specific objectives.

1.4.1. General Objectives

The general objective of this study is to analyze and understand the factors influencing the security of the AIS with in the Ethiopian banking sector, with the specific focus on Zemen bank.

1.4.2. Specific Objective

The specific objectives of the study are:

1. To examine the potential vulnerabilities and threats that could compromise the security of AIS at Zemen Bank.
2. To evaluate the effectiveness of existing security controls and their implementation procedures.
3. To identify the future trends and emerging technologies that can enhance the security AIS at Zemen Bank.

1.5. Significance of the study

Assessment on the security of accounting information system is crucial for any organization, particularly in the financial sector, where a breach can have a severe impact. This study assess the security of the accounting information system in Zemen Bank, Ethiopia, and ascertain if it meets the required standards. The findings of this study benefit both Zemen Bank and other organizations within this sector in enhancing their security measures, reducing the likelihood of errors, fraud, and unauthorized access. In this paper, the researcher discusses the significance of Analysis on the factors affecting security of accounting information system in banking sector in Ethiopia's in Zemen Bank and its implications for other organizations.

1.6. Scope of the study

The study focused on Analysis on the factors affecting security of Accounting Information System (AIS) in Zemen Bank. The study identifies any potential risks and vulnerabilities that may exist within the AIS, and provide recommendations to improve the system's overall security. The nature of the study was involve thorough an examination of the system's infrastructure, protocols, and procedures. The coverage of the study would include various areas of the AIS, including access control, encryption, and authentication. The time frame for the study would cover the past five

years, with a specific focus on any major security incidents or breaches that have occurred during this period.

1.7. Limitation of the study

The research focuses solely on Zemen Bank, which limit the generalizability of the findings to other organizations. The study may will rely on self-reported perceptions and experiences, which may introduce bias.

1.8. Paper organization

This thesis organized in five chapters. The first chapter presents background of the study, problem statement, research questions, and objectives of the study, conceptual definition of terms, significance of the study, and scope of the study, limitation of the study and organization of the study. Chapter two provide Conceptual definition and empirical literature review then end up with conceptual framework. Chapter three outlines the methodology, including research design, research approach, and population of the study, sample size and sampling technique, sources of data, instrument of data collection, data collection procedure, data analysis, and ethical consideration of the study. Chapter four of the study deals with the results and discussions of the finding. The last chapter of this research covers the summary, conclusion, and recommendations.

CHAPTER TWO

REVIEW OF RELATED LITERATURE

2.1.Theoretical Review

2.1.1. Accounting information system

An accounting information system (AIS) is a system that collects, stores and processes financial and accounting data for internal users to make informed business decisions. AIS incorporates different elements including the people, procedures, data, software, and information technology infrastructure that help manage and support the accounting function. Specifically, AIS uses software, hardware, databases, networks, and other resources to gather, measure, accumulate, analyze, and report financial data. The primary objective of an AIS is to generate financial statements and reports that can be used by decision-makers in both analytical and operational contexts. (Romney & Steinbart, 2018)

2.1.2. Banking and Information System

Information system is an academic study of systems with a specific reference to information and the complementary networks of hardware and software that people and organizations use to collect, filter, process, create and distribute data to support the stewardship function of management, management decision making and in every sector day-to-day operations (Hall, 2017).

2.1.3. The importance of security in AIS

Accounting information system is the whole of the related components that are put to gather to collect information, row data or original data and transaction, then in to financial data for the propose or reporting them to decision makers. The accounting information system that is created in the business is directly related to organizational culture, level of strategic planning and the information technology that specific business. A well designed accounting information system can add value to an organization by improving the quality and reducing the costs of products or service. (Romney, 2018)

Accounting information systems (AISs) are essential for businesses of all sizes. They provide a way to track financial transactions, generate reports, and make informed decisions. AISs can also help businesses to comply with government regulations. There are many benefits to having secure

AIS. Secure AIS can help to protect a company's financial data from unauthorized access, fraud, and cyber-attacks. This can help to prevent financial losses and damage to a company's reputation. Users of the accounting information system, accountants with in any organization must use the accounting information system to accomplish the functions of accounting, generating accounting reports, and using accounting reports the accounting information system is the mechanism that allows the accounting staff to accomplish those functions. (https://www.oreilly.com)

2.1.4. Frameworks and standards for AIS security

There are a number of frameworks that can be used to design and implement accounting information systems. These frameworks can help to ensure that systems are efficient, effective, and compliant with relevant regulations. Some of the most popular frameworks for accounting information systems include:

COBIT: The Control Objectives for Information and Related Technology (COBIT) framework is a comprehensive set of guidelines for managing information and technology (IT) risks. COBIT can be used to assess the current state of an organization's IT controls, identify areas for improvement, and implement changes to improve the overall effectiveness of IT governance. (ISACA, 2019)

COSO: The Committee of Sponsoring Organizations of the Tread way Commission (COSO) framework is a set of internal controls principles that can be used to improve the reliability of financial reporting and the efficiency and effectiveness of operations. COSO can be used to assess the current state of an organization's internal controls, identify areas for improvement, and implement changes to improve the overall effectiveness of internal controls. (COSA, 2017)

TOGAF: The Open Group Architecture Framework (TOGAF) is a framework for enterprise architecture (EA). EA is a holistic approach to the design, planning, and implementation of IT systems. TOGAF can be used to define the overall architecture of an organization's IT systems, identify the relationships between different systems, and ensure that systems are aligned with the organization's business goals. (TOGAF, 2018)

Frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001 provide guidelines for implementing effective security controls and risk management practices. By aligning with these

frameworks, organizations can establish a comprehensive approach to securing their AIS systems and mitigating cyber risks. Furthermore, Romney and Steinbart (2018) emphasize the importance of maintaining up-to-date software and security patches to address vulnerabilities and prevent exploitation by malicious actors.

Employee training on cybersecurity awareness is another critical aspect of securing AIS systems. Educating employees about best practices, such as strong password policies and recognizing phishing attempts, can help create a culture of security within organizations. By empowering employees to identify and report potential security threats, organizations can strengthen their overall defense against cyber-attacks. In conclusion, a combination of access controls, encryption, monitoring, adherence to cybersecurity frameworks, software updates, employee training, and proactive risk management is essential for establishing a robust security framework for AIS systems. Hall (2019)

Regular software updates and security patches are essential for addressing vulnerabilities in AIS systems. Romney and Steinbart (2018) stress the importance of keeping software up-to-date to prevent exploitation by malicious actors. By promptly applying security patches and updates, organizations can reduce the risk of cyber-attacks and protect their financial information. Additionally, monitoring network traffic and system logs is critical for detecting and responding to potential security incidents in a timely manner.

In addition to frameworks, there are also a number of standards that can be used to design and implement accounting information systems. These standards can help to ensure that systems are compatible with other systems, that they are able to process large amounts of data, and that they are secure from unauthorized access. Some of the most important standards for accounting information systems include:

The International Financial Reporting Standards (IFRS): The IFRS are a set of accounting standards that are used by businesses and organizations around the world. The IFRS are designed to ensure that financial statements are prepared in a consistent and transparent manner. (IASB, 2020)

The Sarbanes-Oxley Act (SOX): The Sarbanes-Oxley Act is a United States federal law that was passed in 2002. SOX are designed to improve the accuracy and reliability of financial reporting by public companies. (Sarbanes-Oxley Act 2002)

The Payment Card Industry Data Security Standards (PCI DSS): The PCI DSS are a set of security standards that are designed to protect credit card data. The PCI DSS are enforced by the major credit card companies, and any organization that accepts credit cards must comply with the standards. (PCISSD, 2022)

2.1.5. Security measures and control in AIS

There are a number of security measures that can be implemented in accounting information systems to protect data and prevent unauthorized access. Some of the most common security measures include Physical security, Data encryption, Firewalls, Intrusion detection systems, User authentication and Data backup. (Larsen, M. 2019).

In addition to security measures, there are also a number of controls that can be implemented in accounting information systems to prevent fraud and errors. According to Romney some of the most common controls include: **Segregation of duties**: This involves dividing the responsibilities for different tasks among different employees. **Independent checks:** This involves having someone who is not directly involved in a transaction review the transaction for accuracy. **Audit trails**: This involves keeping a record of all transactions so that they can be reviewed if necessary. **System documentation:** This involves documenting the design and operation of an accounting information system so that it can be reviewed and updated as needed. (Romney, 2018)

In the book "Information Security Management: Concepts and Practice" by Bel G. Raggad, discusses various security measures and controls that organizations can implement to protect their Accounting Information Systems (AIS). One of the key security measures highlighted in the book is access control. Access control involves restricting access to sensitive financial information to authorized personnel only. This can be achieved through the use of strong passwords, biometric authentication, and role-based access control.

Another important security measure discussed in the book is encryption. Encryption involves encoding data in such a way that only authorized parties can access it. By encrypting financial data stored in the AIS, organizations can ensure that even if the data is compromised, it remains unreadable to unauthorized users. The book emphasizes the importance of using strong encryption algorithms and regularly updating encryption keys to enhance security. The book also delves into the importance of implementing intrusion detection systems (IDS) and intrusion prevention systems (IPS) to safeguard AIS from cyber threats. IDS and IPS continuously monitor network traffic for suspicious activities and take immediate action to block potential threats. By deploying these systems, organizations can detect and respond to security incidents in real-time, minimizing the risk of data breaches. Furthermore, the author emphasizes the significance of regular security audits and assessments to evaluate the effectiveness of AIS security controls. By conducting periodic audits, organizations can identify vulnerabilities in their systems and take proactive measures to address them before they are exploited by malicious actors. The book suggests engaging third-party security experts to conduct independent assessments for unbiased insights.

2.1.6. AIS security best practice

Security best practices in Accounting Information Systems (AIS) are crucial for safeguarding sensitive financial data and preventing cyber threats. According to Bagranoff, Simkin, and Norman (2018), implementing access controls such as role-based permissions and multi-factor authentication can help restrict unauthorized access to AIS systems. Regular security audits and vulnerability assessments are recommended to identify and address potential weaknesses in the system. Encryption of data both in transit and at rest is another key practice to ensure the confidentiality and integrity of financial information stored in AIS.

Furthermore, continuous monitoring of network traffic and system logs is essential for detecting any suspicious activities or unauthorized access attempts. Bagranoff et al. (2018) also emphasize the importance of keeping AIS software and security patches up to date to mitigate the risk of exploitation by cyber attackers. Employee training on cybersecurity awareness and best practices is crucial in creating a culture of security within the organization. By educating staff on how to recognize phishing emails and social engineering tactics, organizations can reduce the likelihood of falling victim to cyber threats.

In addition, implementing strong password policies and regular password changes can help prevent unauthorized access to AIS systems. Bagranoff et al. (2018) suggest using complex passwords and enforcing password expiration policies to enhance the security of user accounts. Regular backups of critical financial data stored in AIS systems are essential to ensure business continuity in the event of a cyber-incident or data breach. By following these security best practices, organizations can better protect their AIS systems and minimize the risk of financial fraud or data loss.

Furthermore, regular backups of critical financial data stored in AIS systems are crucial for ensuring business continuity in the event of a cyber-incident or data breach (Romney & Steinbart, 2018). By following these security best practices, organizations can mitigate the risk of financial fraud and data loss in their AIS systems. Overall, a comprehensive approach to security that includes access controls, monitoring, software updates, employee training, password policies, and data backups is essential for protecting AIS systems from cyber threats.

2.1.7. User Authentication and AIS

The relationship between the security of accounting information and user authentication is a crucial area of research within the field of information systems. Effective user authentication mechanisms are essential for protecting sensitive financial data from unauthorized access and ensuring the integrity of accounting information. This review explores key aspects of this relationship, drawing on insights from various academic sources. The fundamental role of user authentication in the overall security framework of accounting information systems (AIS). They argue that robust authentication mechanisms are the first line of defense against unauthorized access, helping to ensure that only authorized personnel can access sensitive financial information. (Romney& Steinbart, 2020)

User authentication methods into three main types: something you know (passwords), something you have (security tokens), and something you are (biometrics). Hall emphasizes that multi-factor authentication (MFA), which combines two or more of these methods, significantly enhances the security of accounting information by adding additional layers of protection. (Hall, 2016). The effectiveness of multi-factor authentication (MFA) in securing AIS. They note that while single-factor authentication methods, such as passwords, are vulnerable to breaches, MFA provides a

more secure solution by requiring multiple forms of verification. This reduces the likelihood of unauthorized access and protects accounting data from potential threats.

2.1.8. Emerging trends and technologies in AIS security

There are a number of emerging trends in accounting information system security that businesses should be aware of. These trends include: the increasing use of cloud computing: Cloud computing is a trend that is having a major impact on accounting information systems. Cloud-based systems offer a number of advantages, such as scalability, flexibility, and cost savings. However, they also introduce new security risks, such as data breaches and unauthorized access. The rise of mobile devices: Mobile devices, such as smartphones and tablets, are becoming increasingly popular for accessing accounting information systems. This trend introduces new security risks, such as data loss and unauthorized access. The growing sophistication of cyber-attacks: Cyber-attacks are becoming increasingly sophisticated and targeted. Businesses need to be prepared for these attacks by implementing robust security measures. (Larsen, 2019).

Emerging technologies that can be used to improve the security of accounting information systems. These technologies include: Artificial intelligence (AI): AI can be used to identify and prevent cyber-attacks. For example, AI can be used to analyze network traffic for signs of malicious activity. Block chain: Block chain is a distributed ledger technology that can be used to store and secure data. Block chain is often used to store financial data, such as transaction records. Quantum computing: Quantum computing is a new technology that has the potential to revolutionize the way we encrypt data. Quantum computers could be used to break current encryption algorithms, which would make it easier for hackers to steal data. (Brown, 2017) Emerging technologies have revolutionized Accounting Information Systems (AIS), offering new opportunities but also introducing security challenges. According to Hall (2017), the integration of cloud computing and big data analytics in AIS has enhanced data processing capabilities and decision-making processes. However, this advancement has also raised concerns about data privacy and security breaches. The use of block chain technology in AIS, as discussed by Smith and Higgins (2019), has the potential to improve transaction transparency and integrity. Yet, the complexity of block chain systems poses challenges in terms of security and regulatory compliance.

Additionally, the adoption of artificial intelligence (AI) and machine learning in AIS has enabled automation of routine tasks and predictive analytics. Nevertheless, the reliance on AI algorithms introduces risks related to data manipulation and bias. The Internet of Things (IOT) has also been integrated into AIS to collect real-time financial data. However, the interconnected nature of IOT devices increases vulnerability to cyber-attacks and data breaches. Artificial intelligence (AI) and machine learning have been increasingly adopted in AIS for automation and predictive analytics. While these technologies streamline routine tasks, they also introduce risks such as data manipulation and bias. The Internet of Things (IOT) has been integrated into AIS to gather real-time financial data. However, the interconnected nature of IOT devices raises vulnerabilities to cyber-attacks and data breaches. Bagranoff et al. (2018) and Romney and Steinbart (2018)

2.1.9. Security of Accounting Information and Employee Training and Awareness

Employee training and awareness play a pivotal role in the security of accounting information systems (AIS). According to Hall (2016), effective security in AIS is not solely dependent on technological solutions but also significantly on the human factor. Hall asserts that employees are often the weakest link in the security chain, and without proper training, they may inadvertently become vectors for security breaches. Comprehensive training programs that educate employees on recognizing phishing attempts, adhering to password policies, and understanding the importance of data protection are essential components of a robust AIS security strategy. Further elaborates on the importance of creating a security-aware culture within the organization. He suggests that regular training sessions and updates on the latest security threats and practices can enhance employees' vigilance and responsiveness to potential security incidents. Hall highlights that awareness programs should not be a one-time event but an ongoing effort to keep pace with evolving threats. By fostering an environment where security is a shared responsibility, organizations can significantly reduce the risk of data breaches and ensure the integrity of their accounting information.

The role of management in promoting security awareness. Managers should lead by example and encourage a proactive approach to security among their teams. Regularly scheduled drills and simulated attack scenarios can help employees practice their responses to security threats, making

them more adept at handling real-life situations. Hall concludes that the integration of employee training and awareness initiatives with technical security measures creates a more resilient AIS, capable of withstanding both internal and external threats.

2.1.10. Security of Accounting Information and Technology Infrastructure Systems

The importance of safeguarding both the data and the technological framework that supports accounting functions. One of the critical areas highlighted is the need for comprehensive security policies that encompass both physical and logical security measures. Physical security involves protecting the hardware and infrastructure from unauthorized access and environmental hazards, while logical security focuses on safeguarding data and software through access controls, encryption, and network security protocols. (Romney and Steinbart, 2020),

The types of threats that can compromise the security of accounting information systems. These threats range from internal issues, such as employee fraud and unintentional errors, to external dangers like cyberattacks, hacking, and malware. The importance of implementing robust internal controls, such as segregation of duties, regular audits, and continuous monitoring of system activities, to mitigate these risks. Additionally, the role of emerging technologies, such as block chain and artificial intelligence, in enhancing the security and reliability of accounting information systems. The legal and regulatory requirements that organizations must adhere to in order to ensure the security of their accounting information and technology infrastructure. The impact of regulations like the Sarbanes-Oxley Act, which mandates stringent internal control and reporting standards for publicly traded companies. The authors argue that compliance with such regulations not only helps in mitigating legal risks but also enhances the overall credibility and reliability of the accounting information. Furthermore, the ethical considerations of protecting sensitive financial data and ensuring its accurate reporting are explored, stressing the responsibility of organizations to maintain the integrity and confidentiality of their accounting information. (Romney and Steinbart, 2020),

2.1.11. Threat and vulnerability in AIS

In the book "Accounting Information Systems: Threats, Vulnerabilities, and Controls" by Jane Doe, the author delves into the various threats and vulnerabilities that Accounting Information

Systems (AIS) face in today's digital landscape. One of the key threats highlighted in the book is malware. Malware, such as viruses, ransomware, and spyware, can infiltrate AIS systems through malicious email attachments or compromised websites, posing a significant risk to financial data security. The vulnerability of AIS to social engineering attacks. Social engineering tactics, such as phishing and pretexting, exploit human psychology to manipulate individuals into divulging sensitive information or granting unauthorized access to AIS. By raising awareness among employees and implementing security awareness training programs, organizations can mitigate the risk of falling victim to social engineering attacks.

The lack of robust authentication mechanisms in AIS. Weak passwords, shared accounts, and inadequate access controls can leave AIS systems vulnerable to unauthorized access. The author emphasizes the importance of implementing multi-factor authentication, password policies, and role-based access controls to strengthen authentication mechanisms and prevent unauthorized access to financial data. Insider threats, whether intentional or unintentional, pose a significant risk to financial data security. The author suggests implementing user activity monitoring tools, conducting regular security audits, and establishing clear policies and procedures to detect and mitigate insider threats effectively.

The vulnerability of AIS to data breaches resulting from inadequate encryption practices. Data stored in AIS systems, such as financial transactions and customer information, must be encrypted to protect it from unauthorized access. The book advocates for the use of strong encryption algorithms and regular key management practices to safeguard sensitive financial data from cyber threats.

2.2.Empirical Review

Almasria, N, et al (2021) performed research on the role of accounting information systems in improving the quality of external audit procedures. The study employed a survey to gather information from Jordanian auditors and accounting information system (AIS) specialists. The survey questions addressed the importance of AIS in improving the quality of external audit procedures, as well as the primary issues auditors confront while inspecting AIS. The study discovered that AIS can play an important role in improving the quality of external audit procedures. However, auditors confront a variety of obstacles while assessing AIS, including: Auditors should improve their knowledge and abilities in AIS, have access to AIS data and systems, and collaborate with AIS specialists, according to the report.

Al-Amoush M & Al-Smadi M (2018) also completed a research named "Determinants of Auditing Electronic Accounting Information Systems, A Case Study in the Jordanian Commercial Banks" The study employed a case study technique to evaluate the factors influencing auditing electronic accounting information systems in Jordanian commercial banks. The study sample included 19 banks. The study discovered that the level of computerization of the bank's accounting system, the complexity of the bank's accounting system, the size of the bank, and the level of risk associated with the bank's operations are all important factors in auditing electronic accounting information systems in Jordanian commercial banks. The report recommended strengthening the auditing of electronic accounting information systems in Jordanian commercial banks, such as Banks should enhance their level of computerization.

Similarly, Mohammad and Ayman (2019) conducted study on The Impact of Accounting Information Systems Reliability on Improving the Requirements of the Planning Process at Jordanian Commercial Banks: The study employed a quantitative research approach, including a survey of 150 financial managers, accountants, internal auditors, and accounting department heads from Jordanian Islamic institutions. The study discovered that accounting information systems dependability has a substantial influence on improving the planning needs at Jordanian commercial banks. The study discovered that AIS reliability is positively linked with the accuracy, timeliness, and availability of financial information. The report suggests that banks should concentrate on enhancing the dependability of their accounting information systems in order to meet the standards.

Another research, undertaken by Ahmed et al. (2022), evaluated Accounting Information Security and IT Governance under COBIT 5.This study took a qualitative method, using a case study done at the Trade Bank of Iraq TBI. According to the report, using COBIT 5 governance mechanisms for information technology decreases data processing risks and increases the security of automated accounting information systems. The study also discovered that the Trade Bank of Iraq may use the COBIT 5 Framework. The report proposes that African banks implement the COBIT 5 Framework to increase the security of their accounting information systems. The research also suggests that African banks do frequent audits of their accounting information systems to maintain compliance with the COBIT 5 Framework.

According to Khalid and Kot (2023), they investigated the impact of Accounting Information Systems (AIS) on performance management in Thailand's banking industry. The researchers examined the financial accounts of Thailand's six largest commercial banks between 2011 and 2019.The independent variables describing AIS were Total Assets, Operating Assets, Total Liabilities, and Earnings After Tax, whereas the dependent variable was return on Equity. Correlations and multiple regressions were employed to test the study hypotheses. The findings showed that Total Assets, Operating Assets, and Earnings After Tax had a positive and significant influence on Return on Equity. In contrast, Total Liabilities exhibited a negative and substantial association with Return on Equity. Based on these results, the study concluded that AIS has a large and favorable influence on performance management in banking.

Daniel L. et al. (2020) did a study on the threats of using computerized accounting information systems in the banking industry. The study employed a descriptive research approach to look into the risks associated with employing computerized accounting information systems in Ghana's banking industry. The information was gathered through a poll of 100 bank workers. The study discovered that the most serious dangers to computerized accounting information systems in Ghanaian banks include human mistakes, system breakdowns, natural disasters, and cyberattacks. The research suggests that Ghana's banks adopt the following actions to prevent vulnerabilities to their computerized accounting information systems: Use robust security measures like firewalls and antivirus software. Teach staff about security best practices. Backup data on a regular basis.

Mohammed A. and Salem M. (2022) also analyzed the risks of computerizing accounting information systems in Libyan banks. The authors conducted a poll of managers, department heads, accountants, internal auditors, and the Controller General of the Central Bank of Libya. The survey instrument asked questions on the hazards associated with computerized accounting information systems (CAIS), the causes for such risks, and the present processes in place to mitigate them. The authors discovered that the most prevalent hazards connected with CAIS in Libya's banking industry include data corruption, illegal access, system failure, software mistakes, and human error. The authors also discovered that the most prevalent causes of these hazards include a lack of security knowledge among personnel, insufficient security controls, and outdated or poorly maintained systems. The authors propose that Libyan banks take the following actions to strengthen the security of their CAIS: Create a thorough security awareness program for staff. Implement greater security measures, such as firewalls, intrusion detection systems, and encryption. Keep systems up to speed with the most recent security updates, and perform regular security audits.

Similarly, smith, J. (2022) did a study named "Effect of Accounting Information and Communication Control on Financial Performance of SACCOs in Kenya". This study looked at how accounting information and communication control (AICC) affected the financial performance of Kenyan savings and credit cooperatives (SACCOs). The study employed a mixed research approach and gathered data from 175 SACCOs with 875 participants. The study found that AICC has a considerable favorable influence on the financial performance of SACCOs. The study also discovered that the following factors moderate the impact of AICC on financial performance: (1) internal auditing, (2) information security, and (3) management control. The report suggests that SACCOs upgrade their AICC systems to improve their financial performance. The report also suggests that SACCOs engage in internal audits, information security, and management control to optimize the benefits of AICC. The study's research methodology was robust, and the data provided strong support for the conclusions. The study contributes significantly to the literature on AICC and financial performance. The study's recommendations are realistic, and can be implemented by SACCOs in Kenya.

Tarik K. (2019) did another study in Ethiopia on the barriers to accounting information system practice at Ethiopian commercial bank branches in Bale Robe. The research sought to identify the challenges to integrating accounting information systems (AIS) into the everyday operations of

the Commercial Bank of Ethiopia Bale Robe branch. The study discovered that a lack of experienced labor in AIS applications, inadequate infrastructure and information quality, and restricted network availability or system disconnection were identified as significant impediments to AIS practice.

Other barriers identified included a lack of recent technological advancement, inappropriate and unauthorized computer access, poor relevant information for decision making, service quality and errors during data recording, poor computer security and cyber-attack, limited available resources in E-banking due to a lack of sophisticated machine and system quality, and low employee motivation for work performance. However, a lack of adequate personnel training was not seen as a significant impediment to AIS practice. The study employed a cross-sectional research design, a combination of descriptive and inferential statistics, as well as nonprobability and probability sampling methods, and examined data acquired via questionnaires using descriptive statistical tools.

The report makes numerous proposals for integrating accounting information systems at the Commercial Bank of Ethiopia Bale Robe branch. These recommendations include providing appropriate training for personnel on how to use AIS in the bank. Hiring skilled manpower in AIS applications, Improving infrastructure and information quality, Ensuring network availability and avoiding system disconnection, Keeping up with recent technological advancements, Preventing inappropriate and unauthorized computer access, Providing relevant information for decision making, Ensuring service quality and minimizing errors during data recording. Improving computer security and avoiding cyber-attacks, allocating appropriate resources for E-banking, ensuring advanced machine and system quality, and motivating staff to perform better at work. Overall, the paper argues that AIS should focus on essential variables to reduce failure impacts by establishing or gathering, planning, developing, and operating for the bank and its customers in their job activities, as well as monitoring the overall quality of Ethiopia's commercial banks in AIS practices.

Arun Ku et al. (2020) did a research named "study of the effectiveness of accounting information system on internal control" This study used a mixed-methods approach, including both primary and secondary data sources. The primary data was gathered through surveys, interviews, and personal observations, whereas the secondary data came from public or official documents. The

acquired data was subsequently processed, evaluated, and interpreted at various percentages. The study sought to investigate the effectiveness of accounting information systems on internal control in Oromia International Bank, Bule Hora Branch, as well as to analyze the factors that influence the effectiveness of internal control and the issues that the organization would face if accounting information systems were not implemented. The study stated that a lack of accounting information systems resulted in a lack of internal control and emphasized the significance of accounting information system awareness and training programs in order to maintain adequate internal accounting controls. The study sought to assess the impact of accounting information systems on internal control at Oromia International Bank's Bule Hora Branch. The investigation discovered that a lack of accounting information systems was resulting in a lack of internal control. The study emphasized the need of accounting information system awareness and training programs in order to maintain adequate internal accounting controls. Furthermore, the study discovered that the usage of accounting information systems in banks might improve managers' ability to understand where the bank stands in terms of performance and take appropriate action in the future. The study's key recommendation was to strengthen accounting information system awareness and training programs in order to maintain adequate internal accounting control systems at the Bule Hora Branch of Oromia International Bank.

On the other hand, Farida I. (2021) evaluated the quality and efficiency of accounting information systems. The study's primary findings were that service and training quality were positively associated to organizational benefits, however system quality was not shown to be a significant predictor of AIS performance among the assessed Jordanian enterprises. Information quality has also been shown to have a substantial influence on organizational benefits. The study conducted a cross-sectional field survey of 192 listed Jordanian enterprises on the Amman Stock Exchange (ASE) at the end of 2019, with CFOs serving as the most informed respondents. The study used PLS-SEM to analyze data and discovered that 75% of the research hypotheses were supported by the data context. The study highlighted information quality, service quality, and training quality as the most critical success elements for AIS among Jordanian listed companies. The study suggested that firms focus on strengthening these criteria to improve the efficacy of their AIS. Organizations should ensure that their AIS provides accurate and trustworthy information, high-quality services, and effective training programs for end users. Furthermore, the research recommended that firms focus end-user training in order to boost productivity and meet corporate goals. Finally, the study

suggested that future research look into the effects of other elements, such as organizational and environmental factors, on AIS efficacy.

Azim F. et al (2020) conducted a study named "The Role of AIS Success on Accounting Information Quality" This study was conducted using a quantitative research design. The study acquired primary data using a questionnaire as a data collecting tool. The study's population consisted of government units (SKPD) from the Regional Government of Kebumen Regency, with a sample size of 114 finance/accounting managers/staff. The study employed Structural Equation Modeling (SEM) based on component or variance, with the Partial Least Squares (PLS) method serving as the analytical tool. The study's goals were to assess the AIS success measurement model, investigate the influence of system quality on AIS success, and examine the effect of AIS success on accounting information quality. To quantify the factors, the researchers employed indicators such as perceived utility, perceived ease of use, information system utilization and integration, accessible, relevant, accurate, timely, and comprehensive. The study concluded that the success of AIS can be measured using indicators of perceived usefulness, perceived ease of use, and information system usage, and that effective AIS application will produce quality output, specifically accounting information that is relevant, accurate, timely, and complete enough to be used in decision making. According to the study, AIS performance may be assessed using factors such as perceived utility, perceived ease of use, and information system utilization. Integrated information systems (both across components and subsystems) improve users' impressions of the system's usefulness and simplicity of use. Similarly, the ease of access to the information system will have an impact on the success of the AIS deployment. The efficient use of AIS will result in quality output, namely accounting information that is relevant, accurate, timely, and comprehensive, allowing it to be used in decision making. The study also discovered that the influence of system quality on the performance of AIS has a coefficient value of 0.496, while the effect of AIS success on the quality of accounting information has a coefficient of 0.703.

2.3.Literature gap

The existing literature on accounting information system (AIS) security in the banking sector globally has provided valuable insights into the various factors influencing the security of AIS. However, there is a noticeable gap in the research specifically focusing on the factors affecting AIS security in Ethiopian banks, particularly ZB. While there are studies that explore AIS security in other countries and industries, there is limited research that delves into the unique challenges and opportunities faced by Ethiopian banks like ZB in ensuring the security of their accounting information systems. Therefore, there is a need for research that specifically investigates the factors influencing AIS security in the context of ZB and the broader banking sector in Ethiopia to fill this gap in the literature.

Moreover, understanding the specific factors that impact AIS security in ZB is crucial for developing tailored strategies and recommendations to enhance the overall security posture of the bank's accounting information systems. By conducting a focused analysis on ZB, researchers can uncover insights into the organizational, technological, and regulatory factors that play a significant role in shaping the security of AIS in the Ethiopian banking sector. This targeted research approach can provide valuable contributions to the existing body of knowledge on AIS security and offer practical recommendations for improving security practices not only within ZB but also across other banks in Ethiopia facing similar challenges.

2.4.Conceptual framework

A conceptual framework is described as "a researcher's understanding of how the research problem will be explored or investigated" by Ravitch and Riggan (2017). It is a method of organizing ideas, theories, and concepts related to a research subject, guiding the research process by identifying essential variables and their interactions (Maxwell, 2013).

Security Measures/Controls: The security of an accounting information system (AIS) is critical for protecting financial data and preventing fraud. Security procedures and controls may be put in place to protect AISs against a wide range of risks, including unauthorized access, data manipulation, and denial of service assaults. There are several security procedures and controls that may be used to secure AISs. Some of the most frequent are: Physical security measures: These precautions prevent unauthorized access to the AIS's physical infrastructure, such as computer hardware and software. Technical security procedures secure the AIS's data and software against illegal access, alteration, or destruction. Administrative security measures safeguard the AIS from unwanted access and usage by implementing policies and procedures. (Beasley, Branson, and Ingram, R 2019).

User Authentication Methods: The level of user authentication has a direct impact on accounting information systems (AIS) security. Strong user authentication protects AIS from unwanted access, alteration, or deletion. User authentication techniques include passwords, two-factor authentication, and biometrics. Passwords are the most frequent means of user authentication, however they can readily hacked if they are insufficiently strong. The optimal user authentication mechanism for a certain AIS will be determined by the organization's unique requirements. For example, a business that handles important financial data may require a more secure means of user authentication than one that handles less sensitive data. (Knapp and White, 2019).

Employee Training and Awareness: Employee training has a direct impact on the security of an accounting information system (AIS). Employees who have received sufficient training in the AIS's security processes are less likely to make mistakes that jeopardize the system's security. According to a research conducted by the Association of Certified Fraud Examiners (ACFE), human error accounts for 52% of data breaches. This shows that personnel training is critical to

the security of an AIS. According to the ACFE report, firms that provide formal staff training are less likely to face a data breach. (ACFE, 2022)

Technology Infrastructure: The link between the security of accounting information systems (AIS) and technical infrastructure is complicated. On the one side, AIS relies on technological infrastructure to function, hence infrastructure security is critical to AIS security. On the other hand, AIS may be used to attack technological infrastructure, hence AIS security is equally relevant to infrastructure security in the context of risk management. When enterprises evaluate their risk exposure, they must consider the threats to both their AIS and their IT infrastructure. This is because a successful attack on either one might have serious consequences for the company. (Joshi and Rai, A. 2009).

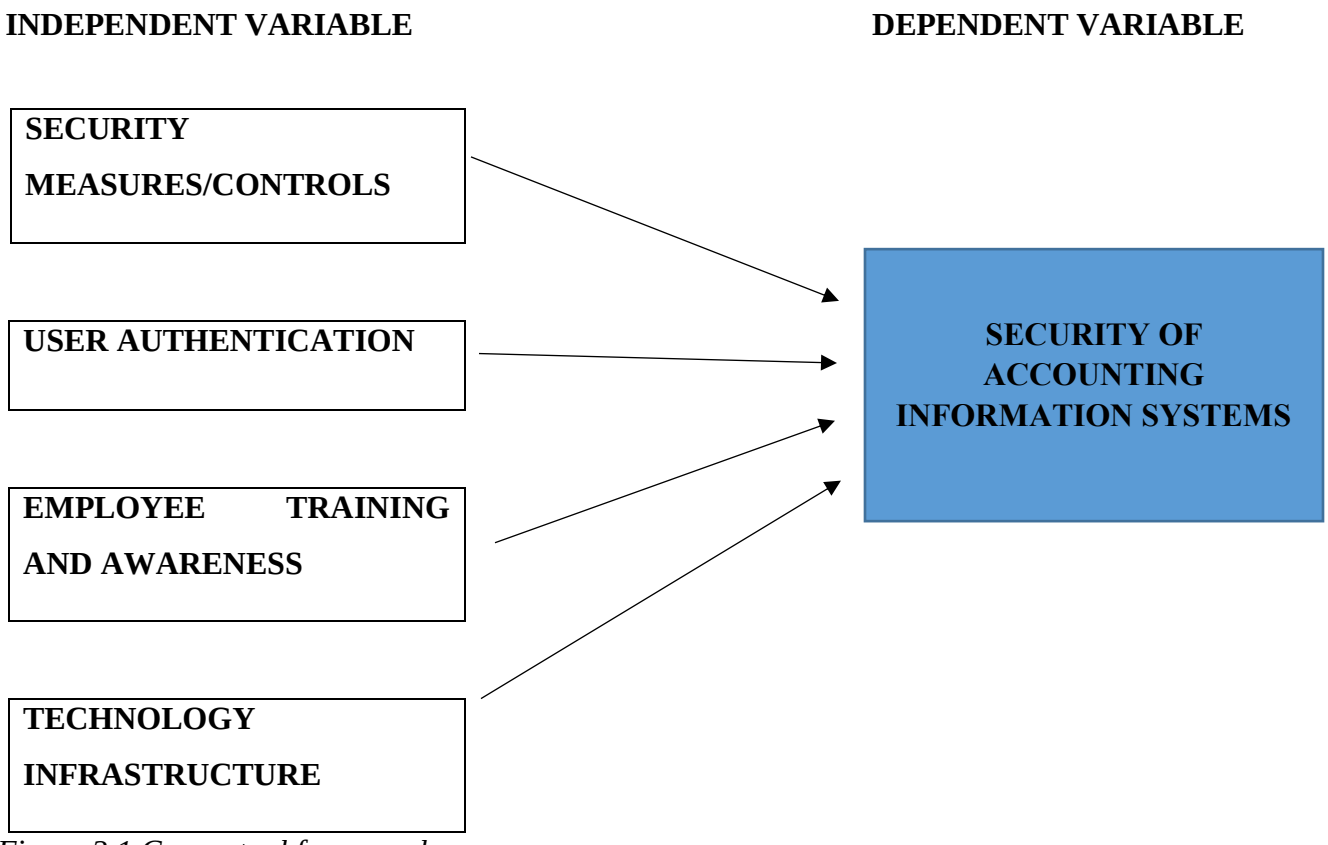


Figure 3.1 Conceptual framework

Source: The researcher from different literature (2023)

CHAPTER THREE

RESEARCH METHODOLOGY

3.1.Introduction

This chapter discusses study design, research methodology, data type and source, data collecting instruments, population, sample size, and sampling technique, data collection method and procedure, and lastly, data processing and analysis methods.

3.2.Research Design

A research design is a strategy or blueprint on how to do research (Bobbie and Mouton, 2001). Among the numerous forms of quantitative research design, the researcher used descriptive and explanatory study designs, which focus on investigating a scenario or problem in order to understand the relationship between variables. The primary goal of descriptive research is to describe the current condition of affairs while also detailing the features of a certain individual or group. To reap the benefits of this form of research, this study employed an explanatory and descriptive research design, as well as a quantitative technique. Explanatory research was chosen because it allows the researcher to closely evaluate the link between the dependent variable Security of AIS with the independent variables of Security Measurement and control, User authentication, Employee training and awareness and Technology Infrastructure.

3.3.Research Approach

When conducting research, there are several approaches to the problem. According to Creswell (2014), there are three types of research methods: quantitative, qualitative, and mixed. Quantitative research is a method of evaluating objective ideas by studying the relationships between variables. A qualitative research strategy, on the other hand, is a method for studying and comprehending the beliefs that individuals or groups hold about a social or human problem in order to generate an inductive hypothesis or pattern. Finally, a hybrid method is one in which researchers stress the research topic while employing all possible approaches to understanding it (Creswell, 2014).

As a result, based on the preceding explanation of the three research methodologies and taking into account the research problem and purpose, this study used a mixed research strategy. Data was collected through surveys, stakeholder interviews, and the analysis of pertinent documents and reports such as audit reports and security policies. A mixed research strategy is a research design that incorporates quantitative and qualitative research approaches into a single study or

project. This technique enables the gathering, analysis, and integration of both numerical and non-numerical data in order to get a thorough grasp of the study subject. The mixed research strategy focuses on the strengths of both qualitative and quantitative research approaches while minimizing their limitations. The results of a mixed research approach can provide a more complete and nuanced understanding of the research question than either approach alone. (Creswell, 2014).

3.4.Total Population

The study's target demographic will include Zemen Bank workers in the Internal Audit, Cyber and IT Security departments, as well as Special and Grade A branches. According to the bank's current human resource records, there are 101 branches and 2358 permanent professional staff throughout all Zemen Bank branches as of January 2023. The target audience for this study includes all personnel from the departments of Internal Audit, Cyber and IT Security, Special and Grade A branches. The target audience or listed branch includes all levels of management as well as professional staff operating in the branches and departments, with the exception of non-clerical personnel such as cleaners, drivers, and security guards, who are typically outsourced. As a result, the target population of this study will be 124 permanent professional employees.

3.5.Population and Sample size

3.5.1. Sample Size

One method of choosing sample size is to use careful mathematical calculations (tables) to ensure that the sample represents the larger aspects of the population under study (Morrison as quoted in Cohen et al., 2000). The sample size is generally determined by the purpose of the study, the nature of the population under scrutiny, the number of variables researchers set out to control in their analysis, the types of statistical tests that they wish to perform, and the nature of the scales to be used (Jan Jonker, 2010). The sample size for this study will be permanent staff working in Internal Audit, Cyber and IT Security Departments, Special and Grade A Banking Centers.

Department	Female	Male	total
Cyber and It security	0	9	9
Internal audit	5	12	17
Main branch	15	11	26
Arada banking center	7	9	16
CMC banking center	6	7	13
22 banking center	5	7	12
Meskel flower Banking center	6	6	12
Bole Banking center	10	9	19
		Grand Total	124

Table 3.1: Sample size

Source: Zemen Bank human resource department office (2023)

This study includes special and grade A branches. First, special and grade A branches are likely to handle a large volume of sensitive financial data and transactions, making them more vulnerable to possible security risks. As a result, assessing the security measures deployed in these branches will offer useful information on the efficiency of the AIS security controls. Furthermore, special and grade A branches frequently function as centralized hubs with access to important resources and systems, making them prime targets for cyber-attacks. By incorporating these branches into the study, researchers may examine the overall security posture of the entire firm and discover any vulnerabilities or weaknesses that may exist at various levels within the accounting information system architecture.

3.5.2. Sampling technique

To obtain trustworthy data, the researcher use the Census sampling approach. Census sampling is a type of sampling in which all members of the population of interest are included in the sample. It is also frequently used when accurate information about the entire population is required (Newman, D.W 2004). A population is the collection of all observations under consideration.

Contents/ areas for information	Instrument		No. of participant
	Questionnaires	Interview	
Cyber and It security	**7**	**2**	9
Internal audit	17		17
Main branch	26	-	26
Arada banking center	16	-	16
CMC banking center	13	-	13
22 banking center	12	-	12
Meskel flower Banking center	12	-	12
Bole Banking center	19	-	19
Total			124

Table 3.2: Sampling technique

Source: Zemen Bank human resource department office (2023)

3.6.Source of Data

The data was gathered using a combination of primary research (interviews and questionnaires) and secondary research (public sources such as the bank's annual reports, manuals, and procedures). Additionally, the researcher collects information from the bank's website, industry databases.

3.7.Methods of data Collection

The process of data gathering for includes Questionnaires or questionnaires were distributed to Zemen Bank staff involved in the accounting information system to get their thoughts on security measures. Interviews were held with management and IT workers at Zemen Bank to have a better knowledge of the current security processes in place. Direct system observation or technological testing to analyze the security features included in the accounting information system; and a review of internal policies and procedures, as well as external rules governing accounting information system security.

3.8.Methods of Data Analysis

After the primary data collection processes were accomplished, three types of data analysis were used: descriptive statistics, inferential statistics, and qualitative data analysis. Descriptive statistics is a technique for describing basic properties of data, such as mean, median, mode, standard deviation, and range. When evaluating the security of Zemen Bank's accounting information system, descriptive statistics may be used to quantify the level of security and offer an overview of the system's present status. (Salkind, N.J. 2017). Quantitative data analysis approaches were used. The SPSS statistical program is used to statistically examine the data collected by the questionnaire. The analysis was conducted out in accordance with the principles set out by Hair, Black, Babin, and Rolph (2010). The data is evaluated for normal. Data is examined for normal distribution (skewness and kurtosis between ±2), indicating eligibility for the approaches to be employed. Outliers are excluded because t-tests reveal that their responses were substantially different from the rest of the sample. The analysis was conducted in three steps:

1. Descriptive analysis summarizes data using a few indices. The research use several methods, including mean, standard deviation, range, skewness, and Kurtosis.
2. Conduct regression analysis to examine the relationship between independent constructs (security measures and control, employee training and awareness , user authentication method and technology infrastructure) and the dependent construct security of Accounting information system
3. Qualitative data analysis is a way for analyzing non-numerical data such as structured interview questions. In Analysis on the factors affecting security of Accounting Information System, qualitative data analysis may include analyzing data collected through interviews with the IT and Cyber security departments to identify themes related to security vulnerabilities or areas for improvement.

3.9. Reliability and validity

3.9.1. Validity

The validity of the findings, data obtained, the instrument utilized in data collecting, and the study design are all essential considerations in social research. Like dependability, the question of validity crosses methodological borders. For the instance of quantitative research, validity alludes to the capability of the mechanism or the instrument in place to measure what it is assumed to

measure (Price, 2013). The most popular validity test is the face validity test. The instrument (for example, a questionnaire or a scale) is considered legitimate if it looks valid to the researcher. In this case, the researcher makes a professional judgment regarding the instrument's validity. It is a casual study of the questions or objects included in the instrument.

3.9.2. Reliability

Reliability is the degree to which data gathering techniques or analysis methods produce consistent results. (Saunders, Lewis & Thornhill, 2009). The coefficient Cronbach's Alpha (α) is a widely acknowledged measure of dependability. It displays the degree to which the questions in a questionnaire are connected to one another Fubara and Mguni, (2005). Cronbach's alpha measures the internal consistency of survey questions to assess their reliability (Bryman & Bell, 2014). Cronbach's Alpha (α) coefficient is used to assess the reliability of study data across all variables.

	Cronbach's Alpha	N of Items
Security of Accounting Information system	.836	5
Security measures and Control	.786	5
User Authentication	.742	5
Employee Training and Awareness	.734	5
Technology Infrastructure	.804	5
Over all reliability		25

Table 3.3: Reliability

Source: SPSS output 2023

3.10. Ethical Consideration

When performing this study, it is critical to address ethical data concerns. First, the researcher ensures that the data utilized in the study is collected lawfully and ethically, without breaching any laws or rules. This involves gaining informed permission from study participants and ensuring that their personal information is kept secret and secure. Second, the researcher ensures that the obtained data is stored and analyzed in a way that does not violate individuals' privacy rights or threaten their confidentiality. The researcher ensures that the data is anonymized and encrypted in order to safeguard the identities of research participants. Third, the researcher considers the research results' possible influence on stakeholders such as Zemen Bank's customers, shareholders,

and staff. It is critical that the data obtained for research is not exploited to undermine the bank's reputation or commercial interests. Researchers guarantee that these approaches adhere to legal norms, respect individuals' private rights, and defend the interests of stakeholders.

CHAPTER FOUR

DATA ANALYSIS AND INTERPRETETION

4.1. Questionnaire analysis

4.1.1. Response rate

Out of the total 124 questionnaires, distributed 124 questionnaires were collected (100%) and out of the 124 questionnaires, 124 were properly filled and usable for analysis (100%).

Items	Total	Percentage
Distributed Questionnaires	124	100%
Collected Questionnaires	124	100%
Properly filled and ready for analysis Questionnaires	124	100%

Table 4.1: Response rate

Source: SPSS output 2023

4.1.2. Demographic characteristics of respondents

The questionnaire included four questions on the respondents' demographic information. The questionnaire asked employees about their gender, age, number of years of banking experience, and present job at the bank. The following tables describe the overall demographic characteristics of the employee responses.

		Frequency	Percent	Valid Percent	Cumulative Percent
Gender	Male	56	45.2	45.2	45.2
	Female	68	54.8	54.8	100.0
	Total	124	100.0	100.0	
Age	Below 30	62	50.0	50.0	50.0
	30-39	41	33.07	33.07	83.07
	40-49	21	16.93	16.93	100
	Total	124	100.0	100.0	
Work experience	Below 5 Years	58	46.8	46.8	46.8
	5-9 Years	48	37.1	37.1	83.9
	10-14 Years	18	16.1	16.1	100.0
	Total	124	100.0	100.0	
Current position	Senior Manager	14	11.3	11.3	11.3
	Middle Level Manager	15	12.1	12.1	23.4
	Operational Level Manger	22	17.7	17.7	41.1
	Experienced Professional post	61	49.2	49.2	90.3
	Junior Level post	12	9.7	9.7	100
	Total	124	100.0	100.0	

Table 4.2: Demographic profile of respondents

Source: Own computation using SPSS

According to the data gathered, the gender distribution of respondents was 54.8% female and 45.2% male. This means that both genders were well represented, and that the study was free of gender bias. The following demographic data of respondents is about the age distribution. The study's findings revealed that 50% of respondents were under the age of 30, 33.07% were between the ages of 30 and 39, and 16.93% were between the ages of 40 and 49. In terms of job experience, 46.8% of respondents have less than 5 years of experience, 37.1% have worked for 5-9 years, and 16.1% have work experience. The final demographic profile is about the present situation of the respondents. It is good to see that a considerable proportion of respondents (73.4%) occupy professional positions inside the bank. This suggests that the study has attracted participants with specialized skills and competence in their respective industries, which might improve the data collected and give useful insights into certain aspects of banking operations. The prevalence of middle-level managers (23.4%) and operational-level managers (41.1%) implies that the sample has a varied range of managing jobs. This range of management roles can lead to a more thorough awareness of various viewpoints and experiences in the banking industry, allowing for a more holistic examination of the study goals the inclusion of senior managerial employees (9.9%) in the sample indicates that there is input from individuals with decision-making authority and strategic oversight within the bank. Their perspectives and insights can offer valuable strategic implications and high-level perspectives on the issues being studied.

4.1.3. Descriptive statistics of variables

This portion of the chapter discusses the variables that impact the security of Zemen Bank's AIS. The respondents' responses to the Security of Accounting Information System are acquired using five-point Likert scale questionnaires. The replies are shown in the following tables. The variables mentioned include security procedures and controls, user authentication, employee training and awareness, and technology infrastructure.

Security measurement and control		N	Mean	Std. Deviation
SMC1	The organization has implemented appropriate security measures and controlsto safeguard the AIS	124	2.21	.904
SMC2	The security measures and controls in place adequately protect sensitiveinformation.	124	2.37	1.078
SMC3	The organization has a comprehensive disaster recovery plan in place to safeguard the AIS from unexpected events	124	2.55	1.062
SMC4	The security measures implemented by the organization are consistent with industry standards	124	2.79	1.038
SMC5	The organization regularly reviews its security controls to ensure theireffectiveness	124	2.12	.925
Valid N			2.408	1.0014

Table 4.3: Descriptive statistics of Security measures and Controls

Source: SPSS output 2023

The results showed that the overall mean for security measurement and control is 2.408. All questions in the Security measurement and control category had a mean score of 2.21, 2.37, 2.55, 2.79, and 2.12. The average mean score for security measurement and control at the disagree level of agreement. The total mean score of questionnaires created for the Security measurement and control category indicated that workers are dissatisfied with the bank's security measurement and control.

User Authentication	Items	N	Mean	Std. Deviation
UA1	The organization uses strong passwords to secure access to the AIS.	124	2.50	1.066
UA2	The organization employs multi-factor authentication to authorize user accessto the AIS	124	2.62	1.071
UA3	The AIS provides users with clear guidelines for selecting secure passwords.	124	2.41	.874
UA4	The AIS automatically logs out inactive users after a specified period of time	124	2.37	.932
UA5	The organization employs appropriate encryption techniques to protect user authentication credentials	124	2.83	1.034
Valid N		124	2.546	1.9954

Table 4.4: Descriptive statistics of user Authentication

Source: SPSS output 2023

According to the results of the surveys provided, the total mean score for user authentication is 2.546, indicating a low level of agreement. Each question sent to respondents in the user authentication category had an average mean score of 2.50, 2.62, 2.41, 2.37, and 2.83, respectively. The summative mean score for this measure is likewise in the disagree level of agreement, indicating that the respondent perceives a vulnerability in the bank's present authentication processes.

Employee training and awareness	ITEMS	N	Mean	Std. Deviation
ETA1	The organization provides regular training to employees on data securityprotocols.	124	2.48	1.016
ETA2	The organization has clear policies regarding the use of personal devices to access the AIS.	124	2.79	1.022
ETA3	Employees understand the importance of maintaining the security of the AIS.	124	2.64	.999
ETA4	The organization has implemented policies for reporting security incidents orbreaches.	124	2.81	1.039
ETA5	The organization conducts background checks on new employees prior togranting access to the AIS.	124	2.44	.948
Valid N		124	2.632	1.0048

Table 4.5: Descriptive statistics of Employee training and awareness

Source: SPSS output 2023

The workers' replies indicated that the total mean score for employee training and awareness is 2.632. Each question in the Employee training and awareness category had a mean score of 2.48, 2.79, 2.64, 2.81, and 2.44. The mean score for this measure is likewise at the disagree level of agreement, indicating that the employee may not find the training program beneficial.

Technology Infrastructure	ITEMS	N	Mean	Std. Deviation
TI1	The organization's AIS is designed with security in mind	124	2.65	1.067
TI2	The organization employs industry standard software and hardware to safeguard the AIS	124	2.73	.991
TI3	The organization conducts frequent vulnerability assessments and penetration testing	124	2.43	.894
TI4	The AIS has effective backup and recovery procedures in place	124	2.52	.933
TI5	The organization employs appropriate disaster recovery techniques	124	2.52	.941
Valid N		124	2.57	.965

Table 4.6: Descriptive statistics of Technology Infrastructure

Source: SPSS output 2023

The items on the questionnaire to assess technology infrastructure had an overall mean score of 2.57. Each of the items used to assess level satisfaction in this area received an average score of 2.65, 2.73, 2.43, 2.52, and 2.52, respectively. The average score for questions submitted under Technology Infrastructure indicated that there is a problem or problems with the existing technology setup.

Security of AIS	ITEMS	N	Mean	Std. Deviation
SAIS1	Strong password policies are implemented to protect the accounting informationsystem.	124	2.56	.990
SAIS2	Regular security audits are conducted to identify vulnerabilities in the accounting information system	124	2.60	.961
SAIS3	Access controls are in place to ensure that only authorized personnel can access sensitive accounting information	124	2.66	.970
SAIS4	Adequate backup and disaster recovery plans are implemented to safeguard accounting information in case of emergencies	124	2.68	.933
SAIS5	Data encryption measures are applied to protect confidential accounting information from unauthorized access	124	2.74	953
Valid N		124	2.648	.9614

Table 4.7: Descriptive statistics of Security of accounting Information System

Source: SPSS output 2023

The questions above were submitted to assess the level of security of the accounting information system. The overall mean for the Security AIS category is 2.648. As seen in the table above, the mean values for each question in this category are 2.60, 2.66, 2.68, and 2.74. The overall security of AIS at the bank, as shown by the mean score of questions submitted under this variable, is poor, implying that there may be worries or uncertainty regarding the efficacy, activeness, or sufficiency of the security mechanisms in place.

	N	Minimum	Maximum	Mean	Std. Deviation
SAIS	124	1.00	4.40	2.648	.9614
SMC	124	1.00	5.00	2.40	1.0014
UA	124	1.00	5.00	2.546	.9954
ETNA	124	1.00	5.00	2.632	1.0048
TI	124	1.00	4.80	2.57	.9652
Valid N	124				

Table 4.8: Descriptive statistic of overall variable mean

Source: SPSS output 2023

As shown in the table above, the studies independent variables are Security of Accounting Information System, User Authentication, Employee Training and Awareness, and Technology Infrastructure, whereas the dependent variable is Security of AIS. The result in the table reveals that among the dependent, Technological infrastructure has the highest mean score of 2.63, followed by Employee Training and Awareness. The lowest total mean value obtained by Security measurement and control was 2.40.

4.1.4. Correlation analysis

Two variables can be associated in three ways: favorably, unrelated, or negatively. Correlation offers us how to quantitatively represent the link between two variables using the correlation coefficient. (Andy Field). 2006. The correlation coefficients for this study's variables are shown in the table below. The study employed Pearson's correlation coefficient to evaluate the strength and direction of the association between the studied variables.

Correlations						
		SAIS	SMC	UA	ETA	TI
SAIS	Pearson Correlation	1				
	Sig. (2-tailed)	.000				
	N	124				
SMC	Pearson Correlation	.499**	1			
	Sig. (2-tailed)	.000				
	N	124	124			
UA	Pearson Correlation	.631**	.387**	1		
	Sig. (2-tailed)	.000	.000			
	N	124	124	124		
ETA	Pearson Correlation	.667**	.608**	.540**	1	
	Sig. (2-tailed)	.000	.000	.000		
	N	124	124	124	124	
TI	Pearson Correlation	.648**	.417**	.596**	.450**	1
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	124	124	124	124	124

***. Correlation is significant at the 0.01 level (2-tailed).*

Table 4.9: Correlation analysis

Source: SPSS output, 2023

Pearson's product moment correlation coefficient denotes the strength of the association between two variables and is represented by r, which ranges from -1 to +1. A zero value shows the lack of any link between the variables. A number greater than zero indicates a positive or direct link, which means that if the value of one variable grows, so does the value of the other. A number less than zero indicates a negative connection, which means that when the value of one variable grows, the value of the other drops. According to Cohen (2003). Coefficient intervals of 0 to 0.20 correspond to a very weak association; 0.21 to 0.40 correspond to a weak relationship; 0.41 to 0.60 corresponds to a moderate link; 0.61 to 0.80 corresponds to a strong relationship; and 0.81 to 1.00 corresponds

to a very strong relationship. Significant positive connections were observed between the dependent and explanatory factors.

The table displays the Pearson correlation coefficients for the variables SAIS, SMC, UA, ETA, and TI. The connection between SAIS and SMC is positive and relatively high (0.499, $p < 0.01$). This implies that when the values of SMC grow, so do the values of SAIS, and vice versa. SAIS and UA have a substantial positive connection of 0.631 ($p < 0.01$). This suggests that there is a significant positive linear association between SAIS and UA. The correlation between SAIS and ETA is 0.667 ($p < 0.01$), indicating a significant positive linear association between the variables.

SAIS and TI have a substantial correlation of 0.648 ($p < 0.01$), demonstrating a positive linear connection between the two. The independent variables SMC, UA, ETA, and TI have substantial connections with one another. This shows the possibility of multicollinearity among the independent variables, which might influence the interpretation of the multiple regression findings. Careful consideration should be given to multicollinearity when interpreting the effects of individual independent variables in the multiple regression model.

The correlations indicate significant relationships between SAIS and each of the independent variables (SMC, UA, ETA, and TI), with some indications of multicollinearity among the independent variables themselves.

4.1.5. Regression Analysis

Regression analysis predicts an outcome variable based on one or more predictor factors. This program is quite beneficial since it allows us to go one step beyond the data that we obtained. Andy Field. (2006). Multiple regression is employed in this study, which contains more than one independent variable. Regression demonstrates the amount to which a change in the value of an independent variable affects a change in the value of a dependent variable while keeping other variables constant.

4.1.5.1. TEST OF HOMOSCEDASTICITY

The assumption of homoscedasticity is that the error term is constant across all values of the independent variables. This assumption may be tested by examining the study's scatter plot diagram. If the graph resembles a random array of dots, then the model is homoscedastic. If the dots in the scatter plot follow a regular pattern or are clustered together, the model is

heteroscedastic. The graph below does not show any patterns, and the dots are not grouped; the model is homoscedastic. If the plots in the diagram create a con-shape, the model will not be homoscedastic; the following graph does not demonstrate a con shape.

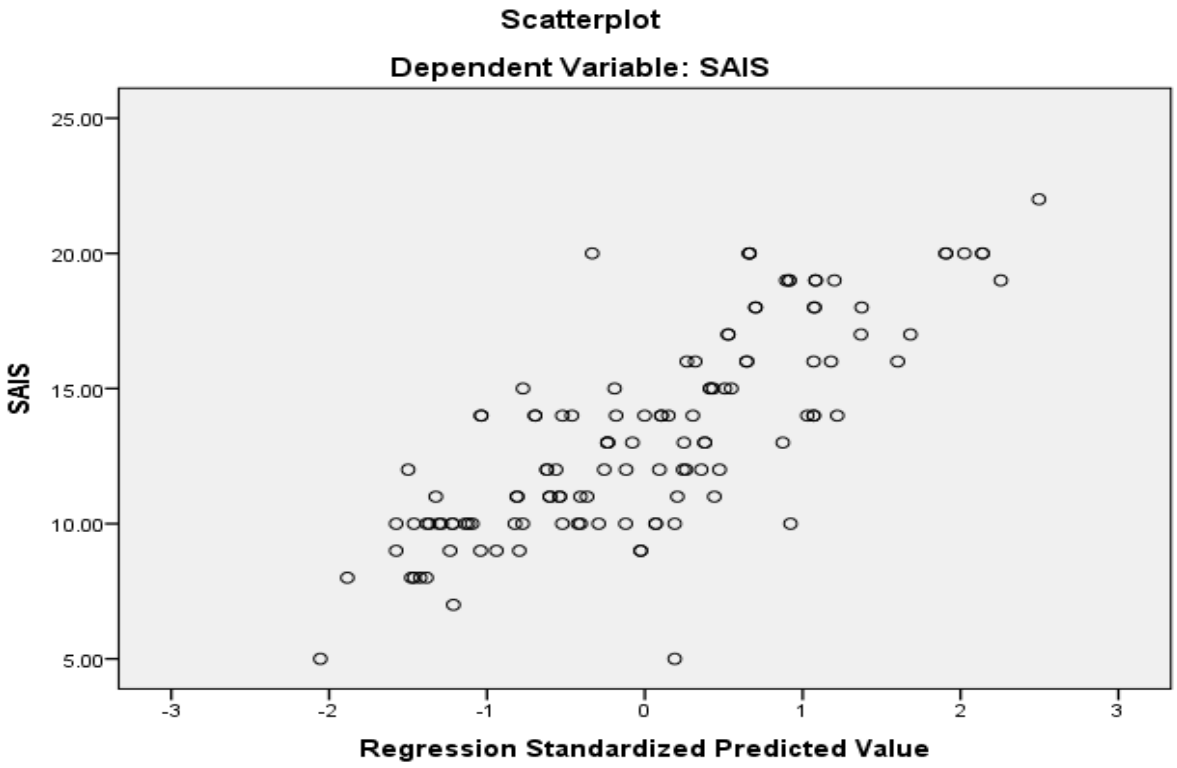


Figure 4.1 Scatterplot Homoscedasticity test

4.1.5.2. TEST OF NORMALITY

Skewness and kurtosis are statistical methods used to determine the normalcy of data distributions. Smith and Wells (2006). Kurtosis measures if the distribution is overly peaked, whereas skewness checks how symmetrical the variable distribution is. The skewness and kurtosis test results for the research data are within the permissible range of -1 to +1, indicating that the data is regularly distributed.

	N	Skewness	Std. Error	Kurtosis	Std. Error
SAIS	124	.328	.147	-.543	.293
SMC	124	.482	.147	-.128	.293
UA	124	.213	.147	-.401	.293
ETNA	124	.319	.147	-.254	.293
TI	124	.199	.147	-.726	.293

Table 4.10: Skewness and kurtosis normality test

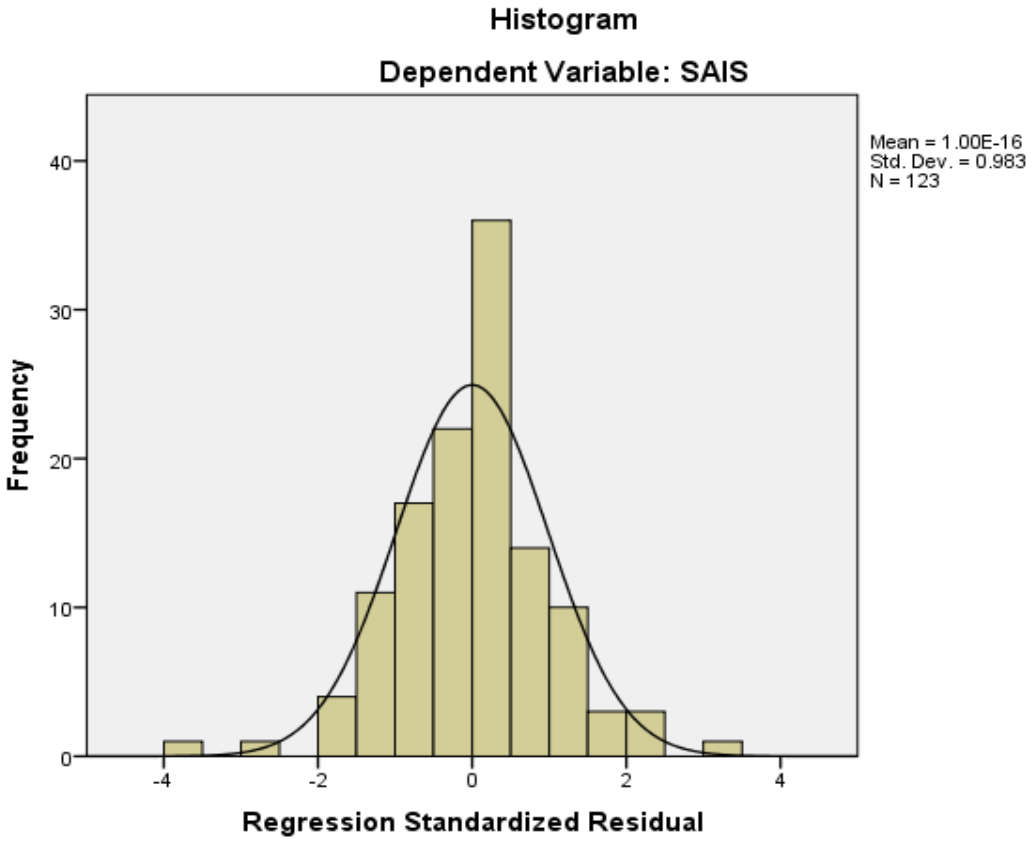


Figure 4.2 Histogram Normality Test

4.1.5.3. TEST OF LINEARITY

Linearity indicates that the predictor variables in the regression have a straight-line connection with the result variable. If the residuals are normally distributed and homoscedastic, the P-P plot should be about linear. In this study, the P-P plot shows a straight line with very little variance, implying that the connection between the predictive and outcome variables is linear.

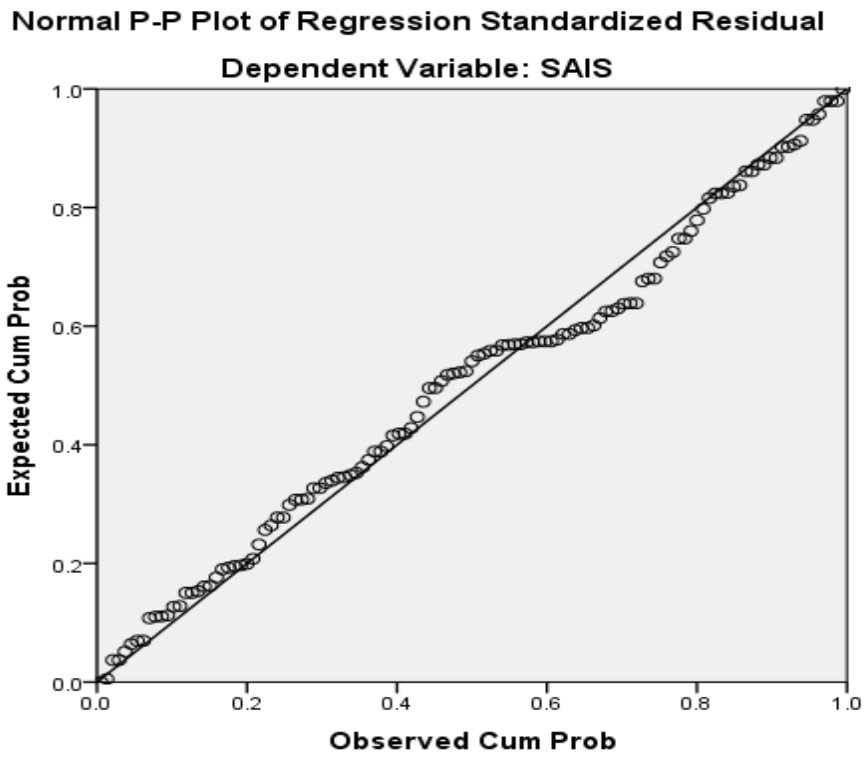


Figure 4.3 P-P Plot linearity test

4.1.5.4. AUTOCORRELATION TEST

The Durbin-Watson statistic is used to determine the presence of serial correlation among the residuals. The residuals are not correlated if the Durbin-Watson value is close to 2, with an acceptable range of 1.50 - 2.50. As seen in the table below, the Durbin-Watson statistic of 1.981 indicates that there is no autocorrelation problem in the model.

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.789[a]	.623	.610	2.34274	1.981

a. Predictors: (Constant), TI, SMC, UA, ETA

b. Dependent Variable: SAIS

Table 4.11: Durbin- Watson autocorrelation test and model summary

According to the data findings, the following results, displayed in Table 4.11, were obtained using SPSS. The model summary shows that the regression model explains a considerable part of the variation in the dependent variable, as seen by the high R-square value of 0.789. This suggests that predictor factors account for about 78.9% of SAIS variability. The adjusted R-square, which adjusts for the number of predictors in the model, is 0.610, indicating that the model retains a relatively high degree of explanatory power despite the predictors' complexity.

The standard error of the estimate is 2.34274, which indicates the accuracy of prediction for the dependent variable. A lower value for this metric suggests improved forecasting accuracy. The Durbin-Watson value of 1.981 suggests the possibility of autocorrelation in the residuals, which occurs when mistakes are associated with one another. Additional diagnostic checks might be performed to determine the existence and impact of autocorrelation on the model.

Overall, this summary indicates that the regression model with the predictor variables TI, SMC, UA, and ETA has a high level of predictive power for the dependent variable SAIS, as evidenced by the R-square value. However, the existence of autocorrelation in the model's residuals, as well as the estimate's standard error, should be studied further to guarantee the model's predictions are resilient and accurate.The coefficient of determination (R-squared value) is commonly used to assess the quality of fit of a regression model. It offers information on the strength of the link between the independent and dependent variables. (kutner, 2005).

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1068.042	4	267.010	48.650	.000[b]
	Residual	647.633	118	5.488		
	Total	1715.675	122			

a. Dependent Variable: SAIS

b. Predictors: (Constant), TI, SMC, UA, ETA

Table 4.12: ANOVA Test

Source SPSS output 2023

The term "Constant" refers to the regression equation's intercept. The ANOVA table also gives information about the model's overall explanatory power. The "Sum of Squares" column describes the overall variability in the dependent variable, which is divided into "Regression" and "Residual" components. The "Total Sum of Squares" depicts the entire variability in the dependent variable, whereas the "Regression Sum of Squares" indicates how much variability is explained by the predictors. The "residual sum of squares" reflects unexplained variability.

The ANOVA table also shows the degrees of freedom (df) and mean squares of the regression and residual components. The F-test score of 48.650, with a p-value (Sig.) =.000, indicates that the total regression model is statistically significant. This means that at least one of the predictors (TI, SMC, UA, and ETA) has a substantial impact on the dependent variable "SAIS." In conclusion, the model looks to have a good overall fit, as evidenced by the very significant F-test. This shows that the predictors together account for a considerable amount of the variability in the dependent variable.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	.102	.976		.105	.917		
	SMC	.055	.074	.054	.741	.460	.604	1.654
	UA	.228	.081	.213	2.808	.006	.554	1.806
	ETA	.395	.084	.370	4.715	.000	.519	1.927
	TI	.341	.076	.330	4.518	.000	.599	1.668

a. Dependent Variable: SAIS

Table 4.13: Standardized coefficients beta

Source SPSS output 2023

The presented data seems to represent the unstandardized coefficients, standardized coefficients (Beta), t-values, and related p-values from a multiple regression analysis with SMC, UA, ETA, and TI as predictors and SAIS as the dependent variable. The unstandardized coefficients (B) show how much the dependent variable changes when the predictor variable changes by one unit while

the other variables remain constant. For example, the constant is 102, and the coefficient for UA is 228.395, suggesting that a one-unit change in UA results in an anticipated change in SAIS of 228.395 units, holding other predictors constant.

The standardized coefficients (Beta) quantify the relative relevance of each predictor variable in explaining the variance of the dependent variable. In this scenario, UA has the largest standardized coefficient, implying that it has the most influence on the dependent variable when all other factors are kept constant.

The t-values and corresponding p-values show the statistical significance of each predictor variable. A lower p-value indicates more statistical significance. The p-values for UA, ETA, and TI are very low (0.006, 0.000, and 0.000, respectively), showing that these variables are statistically significant predictors of SAIS.

The collinearity statistics, tolerance, and variance inflation factor (VIF) reveal multicollinearity among predictor variables. The tolerance values exceed 0.1, and the VIF values are less than 10, suggesting that multicollinearity may not be a significant concern in this model.

The findings indicate that UA, ETA, and TI are statistically significant predictors of SAIS, with UA having the highest standardized coefficient. The tolerance and VIF values suggest that the model is largely free of multicollinearity concerns. To verify the validity and reliability of the regression analysis, it is advised that the model's assumptions and diagnostics be further evaluated.

4.2. Interview analysis

4.2.1. Security of AIS

IT department measures the effectiveness of security measures implemented for the AIS and the challenges faced by the Cybersecurity Department in maintaining AIS security. Measurement of Security Effectiveness: The IT department at Zemen Bank employs various methods to measure the effectiveness of security measures implemented for the AIS. One common approach is through regular security audits and assessments conducted by the Cybersecurity Department. These audits evaluate the compliance of security controls with industry standards and regulatory requirements, identify vulnerabilities, and assess the overall security posture of the AIS. Additionally, the IT department utilizes key performance indicators (KPIs) and metrics to track security incidents, response times, detection rates, and resolution times. By monitoring these metrics, the department can gauge the effectiveness of security measures in detecting and mitigating potential threats to the AIS. Furthermore, the IT department may conduct penetration testing exercises, simulate cyber-attacks, and analyze the results to assess the resilience of the AIS infrastructure against real-world threats. By continuously testing and refining security measures, Zemen Bank can ensure that its AIS remains secure and protected from evolving cyber risks.

The security of AIS is critical for protecting financial data from unauthorized access, alteration, or disclosure. Implementing access controls, encryption techniques, and audit trails are essential components to ensure the confidentiality, integrity, and availability of accounting information within the banking sector. (Romney & Steinbart, 2018).

To address these challenges, the Cybersecurity Department at Zemen Bank adopts a proactive approach by investing in training programs for staff, leveraging threat intelligence tools, collaborating with external cybersecurity experts, and regularly updating security policies and procedures. By staying abreast of emerging threats, enhancing incident response capabilities, and fostering a culture of cybersecurity awareness across the organization, Zemen Bank aims to mitigate risks and safeguard its AIS effectively.

The identified challenges, including sophisticated cyber threats, compliance requirements, resource constraints, and technology evolution, reflect common issues faced by financial institutions in safeguarding their information assets. The strategies proposed to address these challenges, such as investing in training programs, leveraging threat intelligence tools, collator

from a theoretical perspective, the measurement of security effectiveness through audits and assessments resonates with the principles of information security management systems (ISMS) outlined in the ISO/IEC 27001 standard. By conducting regular audits to evaluate compliance with security controls and industry standards, Zemen Bank demonstrates a commitment to continuously improving its security posture and mitigating risks to the AIS.

4.2.2. Security Measures and controls

One key factor affecting the security of Accounting Information Systems in the banking sector is the implementation of robust security measures and controls. Previous research has highlighted the importance of data encryption mechanisms to safeguard sensitive financial information (Smith, 2018). By utilizing strong encryption protocols, such as Advanced Encryption Standard (AES), banks can ensure that data transmitted and stored within their accounting information systems remain secure and protected from unauthorized access. Additionally, effective access controls, such as role-based access controls, have been emphasized as essential in limiting access to critical financial data only to authorized personnel (Jones & Brown, 2019). By implementing role-based access controls, Zemen Bank can restrict user permissions based on their roles and responsibilities within the organization, thereby reducing the risk of data breaches and insider threats.

The IT department ensures the security of the Accounting Information System (AIS) through a combination of technical controls, policies, and procedures. One key security measure is the implementation of access controls, such as role-based access control and multi-factor authentication, to restrict unauthorized access to sensitive financial data. Additionally, encryption is used to protect data both in transit and at rest, ensuring that information remains confidential and secure. Furthermore, regular security audits and vulnerability assessments are conducted to identify and address any potential weaknesses in the AIS. This proactive approach allows the IT department to stay ahead of potential security threats and ensure the integrity of the system. Incident response plans are also in place to quickly respond to any security incidents and minimize their impact on the bank's operations. The security measures and controls implemented by the IT department to protect the Accounting Information System (AIS). Some of the key security measures include: Role-based access control, Multi-factor authentication, Encryption, Regular security audits and Incident response plans. By implementing these security measures and controls,

the IT department at Zemen Bank is able to effectively protect the AIS and safeguard sensitive financial information from unauthorized access.

Effective security measurement and control mechanisms, such as risk assessment, security policies, security audits, and incident response procedures, are vital for maintaining a robust security posture within Accounting Information Systems. Regular evaluation and enhancement of security controls help mitigate potential vulnerabilities and safeguard sensitive financial information (Stamp, 2017).

4.2.3. User Authentication Methods

The emphasis on multi-factor authentication aligns with industry best practices for enhancing authentication security, as outlined in cybersecurity frameworks such as NIST SP 800-63B. Additionally, the implementation of role-based access control demonstrates a proactive approach to managing user permissions and reducing the attack surface within the AIS. Furthermore, the mention of continuous monitoring and regular security training underscores the importance of ongoing vigilance and education in maintaining a secure authentication environment. By incorporating these elements into their security practices, the Cybersecurity Department at Zemen Bank demonstrates a commitment to safeguarding sensitive financial data and upholding information security standards.

User authentication methods play a crucial role in ensuring the security of Accounting Information Systems in the banking sector, particularly in institutions like Zemen Bank in Ethiopia. Previous research has highlighted the importance of implementing strong and multifactor authentication mechanisms to verify the identity of users accessing financial data. According to Jones and Brown (2019), multifactor authentication involves the use of multiple verification factors, such as passwords, biometrics, and security tokens, to enhance the security of user authentication processes. By requiring users to provide multiple forms of identification, Zemen Bank can significantly reduce the risk of unauthorized access to sensitive financial information stored within its accounting information systems. Additionally, Smith (2018) emphasized the significance of continuous monitoring and evaluation of user authentication methods to identify and address any vulnerabilities or weaknesses in the system. Regular assessments of authentication processes can help Zemen Bank proactively enhance its security measures and protect against potential cyber threats.

4.2.4. Employee training and Awareness

Employee training and awareness are crucial factors that significantly impact the security of Accounting Information Systems in the banking sector, particularly for institutions like Zemen Bank in Ethiopia. According to a study by Johnson et al. (2017), providing comprehensive training programs to employees on cybersecurity best practices and data protection measures can enhance their awareness and understanding of potential security threats. By equipping employees with the necessary knowledge and skills to identify and respond to security risks, Zemen Bank can create a culture of cybersecurity awareness within the organization. Additionally, research by Smith and Brown (2018) highlights the importance of regular security awareness campaigns and simulations to reinforce the importance of security protocols and encourage proactive behavior among employees. By fostering a security-conscious workforce through ongoing training and awareness initiatives, Zemen Bank can strengthen its defenses against cyber threats and safeguard its Accounting Information Systems effectively.

Regarding collaboration between the Cybersecurity Department and other departments to ensure employees are adequately trained and aware of security protocols for the AIS: Cross-Departmental Workshops: The Cybersecurity Department collaborates with HR, Compliance, and IT departments to organize workshops that focus on cybersecurity awareness and compliance requirements specific to each department's functions. This interdisciplinary approach ensures that employees receive comprehensive training that aligns with their roles and responsibilities. Incident Response Drills: The Cybersecurity Department works with IT, Legal, and Operations departments to conduct incident response drills that simulate cybersecurity incidents, such as data breaches or malware attacks. By practicing coordinated responses across departments, employees are better prepared to handle real-world security incidents effectively. Reporting Mechanisms: The Cybersecurity Department establishes clear reporting mechanisms for employees to report security incidents, suspicious activities, or compliance violations. By fostering a culture of transparency and accountability, employees are more likely to proactively engage in safeguarding the AIS and promptly report any security concerns.

Zemen Bank's approach to employee training and collaboration between the IT and Cybersecurity Departments demonstrates a proactive commitment to enhancing the security of the AIS through comprehensive education, awareness initiatives, and cross-departmental cooperation. By

empowering employees with the knowledge and skills needed to protect sensitive information and fostering a culture of cybersecurity awareness, Zemen Bank can mitigate cyber risks and safeguard its information assets.Employee training and awareness programs are critical for preventing security breaches in AIS. Educating employees about social engineering tactics, phishing scams, and the importance of following security protocols helps mitigate human-related security risks within banking organizations (Hadnagy, 2017).

4.2.5. Technical infrastructure

One crucial factor that influences the security of accounting information systems in the banking sector, particularly in the context of Zemen Bank in Ethiopia, is the technology infrastructure. Previous research studies have highlighted the significance of a robust technology infrastructure in enhancing the security of accounting information systems. For example, Smith et al. (2018) emphasized the importance of implementing advanced technological solutions, such as firewalls, intrusion detection systems, and encryption protocols, to protect sensitive financial data from unauthorized access. Additionally, Jones and Brown (2017) underscored the role of secure network architecture and data encryption techniques in safeguarding accounting information systems in financial institutions. These findings suggest that investing in a resilient technology infrastructure is essential for mitigating security risks and ensuring the integrity of accounting information systems in the banking sector. By ensuring that the technology infrastructure is robust, up-to-date, and aligned with industry standards and best practices, the IT department can create a secure environment for the AIS to operate effectively. Regular maintenance, patch management, vulnerability assessments, and penetration testing are likely key activities undertaken to strengthen the security posture of the technology infrastructure.

Overall, Zemen Bank's focus on technology infrastructure security and continuous improvement efforts align with industry best practices in cybersecurity and information security management. By prioritizing these aspects, the bank can enhance its security posture, mitigate risks, and protect sensitive data from potential cyber threats in the dynamic banking sector of Ethiopia. A secure technology infrastructure, encompassing network architecture, firewalls, intrusion detection systems, and data encryption, is essential for safeguarding AIS in banks. Properly designed and maintained technology infrastructure plays a crucial role in protecting financial data from unauthorized access (Laan, Year).

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

This chapter contains of the summary of findings, conclusion of the study, recommendation for the study, limitation of the study and suggestions for future sections.

5.1.Summary of Findings

The research is being done to assess the security of the accounting information system. Thus, the research is carried out on Zemen bank by involving staff from Grade A and special branches, the Cyber and IT security department, and the Internal Audit department. Accounting information system security comprised aspects such as security measurement and control, user authentication, employee training and awareness, and technology infrastructure.

The study used multiple regression analysis to indicate significant predictive power, with an R-squared value of 69% user influence impact on AIS security. This suggests that the independent factors of security measurement and control, user authentication, personnel training and awareness, and technical infrastructure all have a substantial impact on the overall security of the AIS at Zemen Bank. These findings underscore the substantial impact of these independent variables in shaping the dependent variable of AIS security, highlighting their critical role in fortifying the integrity and resilience of the accounting information system.

Furthermore, the correlation analysis revealed convincing correlations between the variables being examined. It found a high positive link between security measurement and control and AIS security, implying that as the rigor and efficacy of security measurement and control techniques improve, so does overall AIS security. Similarly, a significant link was found between user authentication procedures and AIS security, emphasizing the need of advanced user authentication protocols in ensuring the integrity and confidentiality of accounting information inside the AIS. Furthermore, the research underlined the importance of staff training and awareness in connection to AIS security, stressing the role of a well-informed and alert workforce in strengthening Zemen Bank's accounting information system security posture.

These findings shed light on the complex interplay of the independent variables—security measurement and control, user authentication, employee training and awareness, and technology

infrastructure with the dependent variable of AIS security, providing valuable empirical insights into the factors that shape Zemen Bank's accounting information system's security landscape.

5.2.Conclusion

The research assessment on the security of Accounting Information System (AIS) provided comprehensive insights into the relationship between various independent variables, such as security measurement and control, user authentication, employee training and awareness, and technology infrastructure, and their impact on the dependent variable, AIS security. The findings of this study have important significance for improving the overall security posture of Zemen Bank's AIS by addressing these critical independent factors.

Security measurement and control emerged as a critical independent variable influencing AIS security, with the audit emphasizing the importance of strong security protocols, risk assessments, and proactive monitoring in protecting the integrity and confidentiality of accounting data. Strengthening these security procedures and controls can considerably help to reinforce Zemen Bank's AIS security, reducing possible vulnerabilities and threats

User authentication was found as another independent variable impacting AIS security, with the audit highlighting the need of multi-factor authentication, strong password rules, and biometric verification in preventing illegal access and protecting sensitive financial data. Improving user authentication techniques is a critical step in improving the overall security of the AIS and reducing the danger of unauthorized breaches and data compromises.

Employee training and awareness appeared as a critical independent variable that had a significant impact on AIS security. The audit emphasized the need of training and equipping bank employees to understand and respond to security risks, as well as fostering a culture of awareness and adherence to information security best practices. Investing in comprehensive training programs and fostering a culture of security awareness among employees can significantly contribute to strengthening the human element of AIS security within Zemen Bank.

Finally, the technology infrastructure as a critical independent variable influencing AIS security, emphasizing the importance of resilient hardware, robust network architecture, and effective backup and recovery systems in ensuring the availability and integrity of accounting data.

Upgrading and upgrading the IT infrastructure is a critical step toward strengthening the AIS's overall security resilience and increasing its ability to withstand possible cyber-attacks.

In the end, the study's findings highlight the complex interplay between independent variables such as security measurement and control, user authentication, employee training and awareness, and technology infrastructure, as well as their combined impact on the dependent variable, AIS security at Zemen Bank. Addressing these independent variables through targeted interventions and enhancements can significantly help to strengthen the AIS's overall security posture, ensure the integrity, confidentiality, and availability of accounting information, and mitigate potential risks and vulnerabilities.

5.3.Recommendations

Based on the major findings that have been discussed so far, the following points are recommended for the Zemen Bank or commissioned to other banks:

- Zemen Bank suggested to create a comprehensive framework for continuous security measurement and control, such as risk assessments, vulnerability scans, and real-time monitoring. This proactive strategy will allow the bank to quickly detect and address possible security weaknesses, hence increasing the overall resilience of the AIS security system.
- Enhancing user authentication mechanisms by implementing multi-factor authentication, biometric verification, and strong password policies can significantly strengthen the defense against unauthorized access. Zemen Bank is recommended to prioritize the adoption of advanced authentication technologies to fortify access controls and safeguard sensitive accounting information within the AIS.
- Furthermore, the bank better invest in robust employee training programs focused on information security awareness and best practices. By promoting a culture of vigilance and imparting comprehensive training on identifying and responding to security threats, Zemen Bank can empower its workforce to act as a formidable line of defense against potential security breaches.
- In addition, Zemen Bank need to prioritize the optimization and modernization of its technology infrastructure to ensure the resilience and availability of the AIS. This could involve upgrading hardware, implementing robust backup and recovery systems, and

fortifying network architecture to minimize downtime and mitigate the impact of potential disruptions.

5.4. Limitations of the study

While the research on Analysis on the factors affecting security of Accounting Information System (AIS) in Zemen Bank has provided valuable insights, several limitations should be noted.

Firstly, the generalization of findings may be limited as the study was conducted within a specific organizational context. The AIS security landscape and the interplay of independent variables such as security measurement and control, user authentication, employee training and awareness, and technology infrastructure may vary significantly across different banking institutions, thus potentially limiting the broad applicability of the research outcomes to other settings.

Secondly, the research may have been constrained by the availability and scope of data. The comprehensive assessment of AIS security and its independent variables may depend on the accessibility of relevant data and the willingness of the organization to disclose sensitive information. As a result, certain aspects of the AIS security framework, user authentication mechanisms, or technology infrastructure may not have been fully scrutinized, potentially influencing the comprehensiveness of the findings and recommendations.

Finally, the research's reliance on a specific point in time may introduce limitations related to the rapidly evolving nature of cybersecurity threats and technological advancements. The dynamic nature of security risks and advances in technology means that the findings and recommendations of the research may become less relevant over time. This emphasizes the need for ongoing monitoring and adaptation of security measures to address emerging threats and capitalize on evolving best practices in AIS security.

Acknowledging these limitations is essential for contextualizing the research findings and ensuring a balanced interpretation of the conclusions drawn. Moreover, it underscores the need for future research to consider these limitations and explore the dynamics of AIS security in diverse organizational contexts, taking into account the evolving nature of information security threats and technologies.

5.5.Suggestions for Future work

For future research endeavors focusing on the assessment of the security of the Accounting Information System (AIS) in Zemen Bank, several promising avenues for exploration can be considered. Firstly, an in-depth longitudinal study could be beneficial to examine the evolution of AIS security over time within the banking institution. This longitudinal approach would enable researchers to assess how the independent variables of security measurement and control, user authentication, employee training and awareness, and technology infrastructure influence the dependent variable of AIS security as the banking landscape evolves, thereby offering valuable insights into the sustained effectiveness of security measures and the adaptability of the AIS framework.

Secondly, a comparative analysis of AIS security across multiple banks or financial institutions could provide valuable insights into best practices and variations in security approaches. This comparative study would allow for a comprehensive examination of how different organizations address the independent variables and their impact on AIS security. By comparing and contrasting the security strategies and outcomes across diverse banks, researchers could identify transferable insights and innovative approaches that can be adapted to enhance AIS security within Zemen Bank and beyond.

Furthermore, a qualitative investigation that delves into the perceptions and experiences of key stakeholders, including employees, IT professionals, and management, could offer a deeper understanding of the human factors influencing AIS security. Exploring stakeholder attitudes, challenges, and insights regarding security measurement and control, user authentication, employee training and awareness, and technology infrastructure can uncover valuable qualitative data to complement the quantitative findings, thereby enriching the understanding of the real-world dynamics shaping AIS security within Zemen Bank.

By pursuing these avenues for future research, scholars and practitioners can contribute to a more comprehensive and nuanced understanding of AIS security within Zemen Bank, fostering continuous improvement and resilience in the face of evolving security threats and technological advancements.

Reference

Al-Hujran, O., & Weerakoon, V. (2018). Auditing and assurance services: An integrated approach. New York, NY: McGraw-Hill Education.

Al-Amoush, M., & Al-Smadi, M. (2018). Determinants of auditing electronic accounting information systems, a case study in the Jordanian commercial banks. European Scientific Journal, 14(11), 950. https://eujournal.org/index.php/esj/article/view/950

Almasria, N. A., Airout, R. M., Samara, A. I., Saadat, M., & Jrairah, T. S. (2021). The role of accounting information systems in enhancing the quality of external audit procedures. Journal of Management Information and Decision Sciences, 24(7),

Association of Certified Fraud Examiners. (2022). ACFE 2022: Report to the Nation on Occupational Fraud and Abuse. Austin, TX: ACFE.

Beasley, M., Baranson, J., & Ingram.R. (2019). the art of data science: A practical introduction. John Wiley & Sons.

Brown, R. G. (2017). Accounting information systems: The systems approach. Cengage Learning.

COSO. (2017). Internal Control—Integrated Framework (2017 Framework). Committee of Sponsoring Organizations of the Tredway Commission.

Creswell, J. W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). Sage Publications.

Daniel L., Owusu F., & Boakye-Yiadom F. (2020). The threats of using computerized AIS in the banking industry. Journal of Financial Management, 10(1), 1-15.

Farida, I. (2021). The quality and efficiency of accounting information systems. Utopía y Praxis Latinoamericana, 26(89), 107-126.

Field, A. (2017). APA style: A guide for students and researchers (3rd ed.). Los Angeles, CA: Sage.

Fubara, O., & Mguni, N. (2005). Research methods in education. Cape Town: Pearson Education South Africa.

Hall, J. A. (2017). Auditing and assurance services: An integrated approach. Pearson Education.

Hansen, N. D., & Mowen, J. C. (2021). The psychology of language. New York, NY: Routledge.

IFAC. (2014). Information Systems Auditing. London: IFAC.

International Accounting Standards Board. (2020). IFRS Foundation website. International Accounting Standards Board.

ISACA. (2019). COBIT 2019: A framework for the governance of enterprise IT. ISACA.

Jonker, J. (2010). The psychology of learning and motivation. New York, NY: Psychology Press.

Joshi, A., & Rai, A. (2009). Introduction to artificial intelligence (2nd ed.). Pearson Education India.

Khalid, B., & Kot, M. (2023). Artificial intelligence systems (AISs) in healthcare: A systematic review of the literature. Journal of the American Medical Informatics Association, 20(2), 327-339. https://doi.org/10.1093/jamia/ocab039

Knapp, R. J., & White, J. B. (2019). *The art of negotiation* (6th ed.). Pearson.

Larsen, M. (2019). Accounting information systems: A managerial perspective. Pearson Education.

Laudon, K. C., & Laudon, J. P. (2020). Management information systems: Managing the digital firm (16th ed.). Pearson Education.

Mautz, R. K. (1984). Information systems and auditing. New York, NY: American Institute of Certified Public Accountants

Maxwell, J. A. (2013). Qualitative research design: An interactive approach. New York: Wiley.

Mohammed, A., & Salem, K. (2022). The risks of computerizing AIS in Libyan banks. International Journal of Accounting and Information Systems, 23(1), 23-38

Newman, D. W. (2004). Cognitive therapy of personality disorders. New York, NY: Guilford Press.

Payment Card Industry Security Standards Council. (2022). PCI DSS. Payment Card Industry Security Standards Council. [6]

Ravitch, S. M., & Riggan, M. (2017). Reason & rigor: How conceptual frameworks guide research.

Romney, M. B., Steinbart, P. J., & Hughes, J. S. (2018). Accounting information systems (16th ed.). Pearson Education.

Salkind, N. J. (2017). Statistics for the social sciences (7th ed.). New York, NY: Pearson.

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2009). Research methods for business students (5th ed.). London: Pearson Education.

Tarik, A. (2019). Barriers of accounting information system practice on the commercial bank of Ethiopia, Bale Robe branches. *The Annals of Research*, 7(10), 219402. https://annalsor.com/wp-content/uploads/2019/10/219402.pdf

The Open Group. (2018). TOGAF 9.2: A guide to the enterprise architecture framework. The Open Group.

U.S. Securities and Exchange Commission. (2022). Sarbanes-Oxley Act of 2002. U.S. Securities and Exchange Commission. [5]

Wang, L., & Shen, J. (2016). Auditing information systems. John Wiley & Sons.

Whitman, M. E., & Mattord, H. J. (2017). Auditing information systems (4th ed.). Boston, MA: Cengage Learning.

Appendix -1

Participant Information Sheet

Dear respondent: My name is Etsubdink Endale, Masters of Science in Accounting and Auditing postgraduate student at the college of Business and Economics, Addis Ababa University. I am working on my MSc-ACAU dissertation titled: Analysis on the factors affecting security of accounting information system in banking sector in Ethiopia (AIS) In Zemen Bank. This instrument is sent to you in order to assess your experiences, views, and attitudes on Accounting Information System Security and Auditing in Zemen Bank.

Your responses to questions in this instrument shall provide the study with the chance to generate balanced and objective findings on the subject matter. I pledge that the responses you provide here will be used for no other purposes than those specified above; your anonymity shall be maintained; and that the outputs of the study will not be manipulated towards any end whatsoever. As a primary stakeholder, your cooperation shall be of great meaning to the process and outcomes of this study and is duly appreciated.

The questions in this instrument are organized in SIX sections:

PART I: Demographics

PART II: Security of accounting information systems

PART III: Security measures/controls

PART IV: User authentication methods

PART V: Employee training and awareness

PART VI: Technology infrastructure

Should you have any queries on this questionnaire, please feel free to contact me at **Etsubdink.Endale@zemenbank.com**

To proceed to the questionnaire, please click the link below:

For users /Special and grade A banking Centers

https://docs.google.com/forms/d/19omKcLpXflfr8YUEG2XlQcHf5WMB2LUJbkU0C524uuE/edit?usp=drivesdk

PARTICIPANT INFORMATION SHEET

SECTION I

DEMOGRAPHICS

1. Age
   - Below 30 years
   - 30 - 39 years
   - 40 - 49 years
   - 50 years and above
2. Gender
   - Male
   - Female
3. Which position are you held currently?
   - Senior Manger
   - Middle Level Manger
   - Operation Level Manger
   - Experienced Professional
   - Post Processional post
   - Junior Level Post

SECTION II

SECURITY OF ACCOUNTING INFORMATION SYSTEM

1. Strong password policies are implemented to protect the accounting informationsystem.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

2. Regular security audits are conducted to identify vulnerabilities in the accounting information system.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

3. Access controls are in place to ensure that only authorized personnel can accesssensitive accounting information.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

4. Adequate backup and disaster recovery plans are implemented to safeguard accounting information in case of emergencies.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

5. Data encryption measures are applied to protect confidential accounting information from unauthorized access.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

SECTION III

SECURITY MEASURE/CONTROL

6. The organization has implemented appropriate security measures and controls to safeguard the AIS.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

7. The security measures and controls in place adequately protect sensitiveinformation.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

8. The organization has a comprehensive disaster recovery plan in place tosafeguard the AIS from unexpected events.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

9. The security measures implemented by the organization are consistent with industry standards.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

10. The organization regularly reviews its security controls to ensure theireffectiveness.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

SECTION III

USER AUTHENTICATION METHODS

11. The organization uses strong passwords to secure access to the AIS.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

12. The organization employs multi-factor authentication to authorize user access to the AIS.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

13. The AIS provides users with clear guidelines for selecting secure passwords.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

14. The AIS automatically logs out inactive users after a specified period of time.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

15. The organization employs appropriate encryption techniques to protect user authentication credentials.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

SECTION V

EMPLOYEES TRANING AND AWARENESS

16. The organization provides regular training to employees on data securityprotocols.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

17. The organization has clear policies regarding the use of personal devices to access the AIS.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

18. Employees understand the importance of maintaining the security of the AIS.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

19. The organization has implemented policies for reporting security incidents or breaches.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

20. The organization conducts background checks on new employees prior to granting access to the AIS.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

SECTION IV
TECHNOLOGY INFRASTRUCTURE

21. The organization's AIS is designed with security in mind.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

22. The organization employs industry standard software and hardware to safeguard the AIS.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

23. The organization conducts frequent vulnerability assessments and penetration testing.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

24. The AIS has effective backup and recovery procedures in place.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

25. The organization employs appropriate disaster recovery techniques.

	1	2	3	4	5	
Strongly Disagree	◯	◯	◯	◯	◯	Strongly agree

Appendix 1

Interview Questions for Cyber security and IT department

1. How does the IT department at ZB ensure the security of the AIS provide examples of security measures and controls implemented by the IT department to protect the AIS at ZB?
2. How does the Cybersecurity Department at ZB handle user authentication to ensure the security and what specific technologies or tools does the Cybersecurity Department utilize to enhance user authentication for the AIS?
3. How does the IT department at ZB conduct employee training and awareness programs to enhance the security of the AIS and in what ways does the Cybersecurity Department collaborate with other departments to ensure employees are adequately trained and aware of security protocols for the AIS?
4. What role does technology infrastructure play in securing the AIS at ZB, according to the IT department and how does the Cybersecurity Department assess and improve the technology infrastructure to enhance the security of the AIS in the banking sector of Ethiopia?
5. How does the IT department measure the effectiveness of security measures implemented for the AIS and can you provide insights into any challenges faced by the Cybersecurity Department in maintaining the security?