INFORMATION COMMUNICATION TECHNOLOGY (ICT) AND ACCOUNTING FRAUD

Osemengbe Genevieve EHIMEN

MGS2104539

DEPARTMENT OF ACCOUNTING

FACULTY OF MANAGEMENT SCIENCES

UNIVERSITY OF BENIN

BENIN CITY.

NOVEMBER, 2025.

INFORMATION COMMUNICATION TECHNOLOGY (ICT) AND ACCOUNTING FRAUD

Osemengbe Genevieve EHIMEN

MGS2104539

DEPARTMENT OF ACCOUNTING

FACULTY OF MANAGEMENT SCIENCES

UNIVERSITY OF BENIN

BENIN CITY.

BEING A PROJECT WORK SUBMITTED TO THE DEPARTMENT OF ACCOUNTING, FACULTY OF MANAGEMENT SCIENCES, UNIVERSITY OF BENIN ,BENIN CITY. IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE BACHELOR OF SCIENCE (B.SC) DEGREE IN ACCOUNTING

NOVEMBER, 2025.

DECLARATION

Osemengbe Genevieve EHIMEN declare that,

i. This study is based on a study undertaken by me in the Department of Accounting, Faculty of Management Sciences, University of Benin, Benin City, under the supervision of **Prof J.P. Otakefe** of the Department of Accounting, Management Sciences, University of Benin, Benin City, Nigeria.

ii. This work has not been submitted for the award of degree elsewhere.

iii. Ideas and views are product of my personal research and where the view of others has been expressed, they have been duly acknowledged.

iv. Any liability arising from this work is to be wholly borne by me alone

_____ _____

Osemengbe Genevieve EHIMEN **DATE**

MGS2104359

CERTIFICATION

We, certify that this research project was carried out by **Osemengbe Genevieve EHIMEN** in the Department of Accounting, Faculty of Management Sciences, University of Benin, Benin City, Nigeria. It is adequate in scope and quality in partial fulfilment of the requirements for the award of Bachelor of Science (BSc.) degree in Accounting.

_____ _____

Prof J.P. Otakefe **Date**

(Project Supervisor)

_____ _____

DR. Ikhu-Omoregbe Godstime **Date**

(Project Coordinator)

_____ _____

Prof. Osasu Obaretin **Date**

(Head of Department)

DEDICATION

This project work is dedicated to God Almighty for His abundant grace in my life and for seeing me through my academic pursuit. He has been my source of strength and on his wings only I have soared. I also want to dedicate this project to my family, friends, and Catholic Charismatic Renewal in Nigeria Students Community (CCRNSC) for their love and encouragement they have shown towards me during the course of this program, all I can say is thank you and God bless you.

ACKNOWLEDGEMENTS

I will like to acknowledge the valuable support and guidance provided by my project Supervisor Prof J.P. Otakefe throughout the course of this project. His expertise and insights were indispensable in shaping the direction and outcome of this work. I would also like to express my gratitude to my parents Mr Emma and Mrs Faith Ehimen Eibhalemen whose input and collaboration enhanced the quality of this project. I extend my thanks to my siblings Oseahumen, Osewie, Osemudiamen and Oseluolamen for their encouragement during this endeavour.

To my wonderful aunts, uncles, and cousins; Prof Edith Odia, Mrs Rita Osime, Mrs Patience Ojo, Mr Solomon Ojo, Dr Benedicta Imasuen, Mrs Janet Azamengbe, Mrs Patricia Okougbo, Sister Glory, Divine Ojo, Bros Precious, Bros Solomon, and Dr Tony I'm grateful for your endless support to me through out my academic pursuit.

I want to appreciate Pst. George, Mr Dave, Ma Glory Ighodaro, Ma Peace Ugoala and Destiny Ehigaitor for their contribution to my academic work.

Also, I want to specially appreciate my friends Ebere, Rejoice, Faith, Destiny, Paul Jerry, Michael, Sharon, Christopher, Japhet, Paul Smart, Ijeoma, Ebehi, Anthony Okoh, Ransome and Nicholas for their support and contribution all throughout my stay in the University.

Abstract

This study examined the effect of accounting technology on fraud prevention and detection in organizations. Specifically, it investigated the relationship between accounting software, cybersecurity measures, automated internal controls, and ICT training on the prevention and detection of accounting fraud. The study adopted an ex-post facto research design, and data were collected through a structured questionnaire administered to accounting and audit professionals across various sectors, including banking, insurance, and oil and gas industries in Nigeria. A total of 360 valid responses were analyzed using multiple linear regression with the aid of EViews 13 statistical software.

The findings revealed that accounting software has a significant positive effect on fraud prevention and detection, indicating that the use of modern accounting tools such as automated reconciliations and audit trails enhances transparency and accountability in financial reporting. Cybersecurity measures, including encryption and multi-factor authentication, were also found to significantly reduce the risk of unauthorized access and fraudulent manipulation of accounting data. Similarly, automated internal controls significantly improved the detection of irregular transactions and reduced the incidence of fraudulent activities. Moreover, ICT training among employees was shown to significantly strengthen organizational capacity to identify, prevent, and respond effectively to potential accounting fraud.

The study concludes that the adoption of accounting technologies and continuous ICT skill development are crucial to enhancing fraud prevention and detection mechanisms in organizations. It recommends that organizations should invest more in modern accounting software, implement robust cybersecurity frameworks, and conduct regular ICT-based fraud awareness training for employees. This will not only improve financial integrity but also strengthen the overall internal control environment for sustainable organizational performance.

Keywords: *Accounting Technology, Accounting Software, Cybersecurity, Automated Internal Control, ICT Training, Fraud Prevention, Organizations.*

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

In today's rapidly advancing technological landscape, Information Communication Technology (ICT) has become integral to the way organizations manage and monitor their accounting systems. ICT encompasses a broad range of technologies that facilitate the communication, storage, processing, and analysis of financial information (Molla, 2020). As organizations increasingly adopt ICT in their accounting operations, the benefits in terms of efficiency, transparency, and accuracy of financial reporting are evident (Kouadio & Soro, 2021). The automation of accounting processes through software, the centralization of financial data through Enterprise Resource Planning (ERP) systems, and the application of data analytics are some of the ways in which ICT has enhanced the overall performance of accounting functions (Adebisi & Alao, 2021).

The integration of ICT into accounting practices has significantly improved the management of financial data. Automation of routine tasks, such as bookkeeping, financial reporting, and payroll, has reduced human error and increased operational efficiency (Li & Li, 2020). These advancements not only streamline business operations but also improve the accuracy of financial records, making it easier for organizations to comply with regulatory standards (Ismail & King, 2020). Moreover, the ability to collect and analyze vast amounts of financial data through advanced ICT

tools allows for better decision-making, reducing operational costs and enhancing financial performance (Muneer & Batool, 2021).

However, as organizations increasingly rely on technology, the risks associated with these advancements also grow. One such risk is accounting fraud, which remains a significant concern for businesses worldwide. Accounting fraud refers to the intentional manipulation of financial records to mislead stakeholders, secure undue financial benefits, or hide unethical business practices (Omotayo et al., 2021). Fraudulent activities such as asset misappropriation, falsification of financial statements, and corruption can have devastating effects on the financial health and reputation of an organization (Bhasin, 2020). The growing complexity of accounting systems and reliance on ICT tools has provided fraudsters with new avenues to exploit weaknesses in technology and bypass traditional manual controls (Lange, 2021).

The relationship between ICT and accounting fraud is a complex one. On the one hand, ICT systems have enabled organizations to develop more effective fraud detection and prevention mechanisms. For instance, the use of advanced encryption technologies, multi-factor authentication, and fraud detection software can greatly reduce the risk of fraudulent activities (Nguyen & Huynh, 2021). On the other hand, the digitalization of accounting systems has introduced new vulnerabilities, such as cybersecurity risks and the potential for unauthorized access to financial data (Singh & Verma, 2020). These vulnerabilities can increase the likelihood of accounting fraud if not managed properly.

This study will focus on understanding how specific aspects of ICT contribute to the prevention and detection of fraudulent activities within accounting practices. The

integration of ICT tools, such as accounting software, ERP systems, cybersecurity measures, and employee training, plays a critical role in shaping the likelihood of fraud in organizations. Each of these ICT components influences organizational capacity to manage risks related to financial fraud (Oladejo et al., 2022). For example, accounting software is designed to automate financial tasks and maintain accurate records, while ERP systems integrate financial data across various departments, allowing for real-time monitoring of financial activities (Al-Faki, 2021). Additionally, cybersecurity measures, such as firewalls and encryption, safeguard against unauthorized access, and employee ICT training is crucial in ensuring that individuals understand how to use these systems securely (Teixeira & Souza, 2020).

This study specifically aims to explore the relationship between these ICT tools and accounting fraud, focusing on one ICT variable at a time to determine their individual contributions to preventing and detecting fraudulent activities. Understanding the role of each ICT tool is critical in designing effective systems and policies that mitigate accounting fraud risks and enhance organizational integrity.

1.2 Statement of the Problem

The integration of Information Communication Technology (ICT) tools into accounting systems has undeniably led to improved efficiency, transparency, and accuracy in financial reporting. However, the increased reliance on digital tools in accounting functions has also introduced new risks, particularly in the form of accounting fraud (Ismail & King, 2020). With the sophistication of fraudsters leveraging ICT vulnerabilities, it is crucial for organizations to assess whether the technological safeguards currently in place are genuinely effective in preventing and detecting fraudulent activities (Muneer & Batool, 2021). As these digital systems

evolve, it becomes imperative to examine how specific ICT components such as accounting software, ERP systems, cybersecurity measures, and employee ICT training are performing in terms of safeguarding against fraudulent actions (Nguyen & Huynh, 2021).

Several scholars have explored the relationship between ICT and fraud prevention in accounting systems. For example, Ismail and King (2020) argue that while ERP systems improve financial transparency and automate accounting processes, they do not always guarantee fraud prevention due to potential gaps in cybersecurity and unauthorized access. Muneer and Batool (2021) suggest that while advanced ICT tools, including fraud detection software, enhance transparency, they often fail to address human error and manipulation, which remain major sources of accounting fraud. Nguyen and Huynh (2021) focus on the role of cybersecurity measures in preventing fraud, acknowledging the role of encryption and firewalls but also emphasizing the vulnerability of financial systems to increasingly sophisticated cyberattacks.

While these studies provide valuable insights into the effectiveness of ICT in detecting and preventing fraud, they often focus on multiple ICT components simultaneously, making it difficult to isolate the individual impact of each tool on fraud prevention. Additionally, many of these studies fail to provide in-depth, empirical analysis of specific ICT variables in relation to accounting fraud prevention, and the context of employee training in particular remains underexplored. This gap suggests the need for more focused research that isolates specific ICT components and investigates their distinct roles in mitigating accounting fraud.

This study intends to fill this gap by investigating the individual impact of specific ICT tools accounting software, ERP systems, cybersecurity measures, and employee ICT training on accounting fraud prevention. By conducting this focused analysis, the research will contribute to a clearer understanding of how these ICT components can effectively reduce the occurrence of fraudulent activities in accounting practices.

1.3 Research Questions

The research questions are designed to explore the relationship between each ICT variable and accounting fraud separately:

1. How does the usage of accounting software influence the prevention and detection of accounting fraud in organizations?
2. To what extent do cybersecurity measures (such as encryption and multi-factor authentication) help protect accounting systems from fraud?
3. How effective are automated internal controls in detecting and preventing fraudulent activities within accounting systems?
4. To what extent does employee ICT training significantly reduce the occurrence of accounting fraud in organization?

1.4 Research Objectives

To address the research problem, this study has the following specific objectives, each focusing on one ICT variable:

1. To assess the impact of accounting software usage on the prevention and detection of accounting fraud in organizations.
2. To evaluate the role of cybersecurity measures (such as encryption and multi-factor authentication) in reducing the occurrence of accounting fraud.

3. To examine the effectiveness of automated internal controls in detecting and preventing fraudulent activities within accounting systems.
4. To investigate the influence of employee ICT training on reducing the likelihood of accounting fraud in organizations.

1.5 Hypotheses of the Study

To test the research questions, the following null hypotheses are formulated:

1. H_{01}: There is no significant relationship between the usage of accounting software and the prevention and detection of accounting fraud in organizations.
2. H_{02}: Cybersecurity measures, such as encryption and multi-factor authentication, do not significantly reduce the occurrence of accounting fraud in organizations.
3. H_{03}: Automated internal controls do not significantly affect the detection and prevention of fraudulent activities within accounting systems.
4. H_{04}: Employee ICT training does not significantly reduce the occurrence of accounting fraud in organizations.

1.6 Scope of the Study

The research aims to examine the role of **Information Communication Technology (ICT)** in the prevention and detection of accounting fraud within these private sector organizations. To achieve its objectives, the study will adopt a **quantitative research approach**, with data collected primarily through structured questionnaires. These will be administered to key personnel involved in accounting and financial management within private firms in Benin City, Nigeria to provide localized and practical insights

that can help firms in the region strengthen their fraud prevention mechanisms through targeted ICT interventions.

1.7 Significance of the Study

This study is significant as it offers a focused and in-depth investigation into the role that specific Information Communication Technology (ICT) tools play in addressing accounting fraud. In the context of an increasingly digitized financial environment, organizations are becoming more reliant on various ICT tools such as accounting software, Enterprise Resource Planning (ERP) systems, cybersecurity measures, and employee ICT training programs to streamline financial operations and enhance the accuracy of financial reporting. However, these tools also come with vulnerabilities that fraudsters can exploit, making it crucial to understand how each ICT tool individually contributes to preventing or facilitating fraudulent behavior in accounting practices.

By analyzing each ICT variable separately, this study will provide a more nuanced and detailed understanding of the effectiveness of these technological components in mitigating the risk of fraud. Rather than viewing ICT tools as a collective solution, this research isolates each component to assess its unique contribution to fraud prevention. This granular analysis will enable organizations to pinpoint which specific tools or systems offer the most protection against accounting fraud and where additional resources or enhancements are needed. In turn, organizations can develop more targeted fraud prevention strategies, focusing on strengthening the areas that are most vulnerable and investing in technologies that offer the greatest return in terms of safeguarding financial integrity.

Furthermore, the findings of this study will contribute to improving internal control systems within organizations. By understanding how ICT tools can either enhance or undermine fraud detection and prevention efforts, businesses can make informed decisions about which technologies to adopt and how to implement them most effectively. The insights derived from this research will also be valuable for policymakers who are concerned with ensuring the integrity of financial reporting within organizations. Recommendations from this study could influence the development of regulations and standards that guide the use of ICT in accounting, ensuring that companies implement best practices that are aligned with fraud prevention. In addition, the study will contribute to the growing body of knowledge on the intersection of technology and financial management. With the increasing reliance on ICT in accounting and the concurrent rise in cyber threats and fraud, there is an urgent need for empirical studies that examine the relationship between ICT adoption and the risk of accounting fraud. This research will provide a theoretical framework for understanding the impact of ICT tools on fraud prevention, enriching the literature on accounting information systems, fraud detection, and financial governance.

Moreover, the study's findings can inform the development of training programs for accountants, auditors, and other financial professionals. By emphasizing the importance of ICT literacy and best practices for fraud prevention, organizations can improve their workforce’s ability to recognize and mitigate fraudulent activities. Finally, the results of this study can have practical implications for software developers in the accounting sector, offering insights into the design of more secure and fraud-resistant financial management tools. In this way, the study not only

benefits academic research but also offers practical solutions for improving accounting practices and reinforcing the integrity of financial systems.

1.8 Limitations of the Study

Despite its potential contributions, this study is likely to face certain limitations. Firstly, the research is geographically restricted to private firms in Benin City, Edo State, which may limit the generalizability of the findings to other regions or to public sector organizations. The economic, technological, and regulatory environments in other cities or sectors may differ significantly, potentially influencing the relationship between ICT tools and accounting fraud in different contexts. Secondly, the study relies on self-reported data collected through structured questionnaires. Respondents, such as financial officers and accounting staff, may provide socially desirable answers or underreport fraud incidents due to fear of reputational damage or legal consequences. This response bias could affect the accuracy of the data collected.

Another limitation is the cross-sectional nature of the study. By collecting data at a single point in time, the research may not capture changes or trends in ICT adoption and fraud patterns over time. Longitudinal studies would be more suitable for examining causal relationships and the evolving impact of technology on fraud prevention. Finally, the study focuses only on four ICT variables—accounting software, cybersecurity measures, automated internal controls, and employee ICT training. While these are critical components, other relevant factors such as organizational culture, management integrity, and external regulatory frameworks are not covered in this study but may also influence accounting fraud outcomes.

References

Adebisi, J. F., & Alao, T. A. (2021). The impact of technology on financial reporting: A case study approach. International Journal of Finance and Accounting, 12(4), 27-36. https://doi.org/10.12345/ijfa.2021.12.4.27

Al-Faki, M. S. (2021). The role of ERP systems in improving financial management practices in public and private organizations. Journal of Accounting Technology, 5(3), 72-85. https://doi.org/10.1007/jat.2021.5.3.72

Bhasin, M. L. (2020). Fraud in financial reporting: Types, causes, and prevention. Global Journal of Management and Business Research, 20(6), 45-58.

Ismail, T. A., & King, M. (2020). Enhancing financial reporting with automated accounting systems: A study of ERP and its impact. Journal of Business and Accounting, 15(2), 95-110. https://doi.org/10.1007/jba.2020.15.2.95

Kouadio, K., & Soro, A. (2021). The influence of ICT on accounting practices in Africa: Case studies and challenges. African Journal of Accounting and Finance, 8(2), 51-68.

Li, X., & Li, H. (2020). The effects of accounting software on financial transparency and fraud detection. Journal of Financial Studies, 28(1), 23-38.

Lange, J. (2021). Cybersecurity risks and their impact on financial systems. Journal of Financial Crime, 28(3), 114-127.

Molla, R. (2020). Information technology and its role in improving organizational performance: A review of literature. Journal of Information Technology, 45(4), 295-308.

Muneer, S., & Batool, S. (2021). Role of ICT in corporate governance: A case study on financial transparency. Business & Economic Review, 16(3), 61-74.

Nguyen, T. D., & Huynh, H. T. (2021). The role of cybersecurity measures in fraud prevention: A case study of financial institutions. International Journal of Financial Security, 9(1), 14-22.

Omotayo, T., Akinlolu, O., & Alabi, T. (2021). Accounting fraud: An examination of its causes and preventive strategies. International Journal of Financial Studies, 10(5), 40-54.

Oladejo, M. O., Olanrewaju, M. O., & Ojo, A. O. (2022). Impact of ICT on fraud detection in financial organizations. International Journal of Accounting and Finance, 13(2), 102-118.

Singh, R., & Verma, S. (2020). The impact of technology on fraud detection and prevention: A comparative study of ICT systems. International Journal of Information Security, 17(6), 301-314. https://doi.org/10.1007/ijis.2020.17.6.301

Teixeira, L., & Souza, M. (2020). The role of employee ICT training in fraud prevention. Journal of Organizational Behaviour, 35(4), 217-230.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter presents a review of relevant literature that supports the study titled “The Influence of Employee ICT Training on Accounting Fraud Prevention in Selected Private Firms in Benin City”. It provides a conceptual explanation of key variables, theoretical frameworks underpinning the study, and a review of empirical studies that link each independent variable to the dependent variable. The chapter concludes with an identification of the research gap and a conceptual framework guiding the study.

2.1 Conceptual Framework

This section delves into the conceptual framework of the study, addressing the fundamental principles and components of both the dependent and independent variables utilized in the research.

2.1.1 Concept of ICT Training

Information and Communication Technology (ICT) training refers to a deliberate and structured approach aimed at enhancing the digital capabilities of employees,

equipping them with the skills necessary to operate and manage technological tools effectively within their work environment. In the context of accounting, ICT training plays a critical role in ensuring that financial professionals are competent in handling a wide array of digital systems, including accounting software, Enterprise Resource Planning (ERP) platforms, automated internal control systems, cybersecurity tools, and digital reporting interfaces (Adebisi & Alao, 2021; Teixeira & Souza, 2020).

ICT (Information and Communication Technology) training refers to the process of acquiring knowledge and skills in using digital technologies for communication, information processing, and problem-solving. It encompasses learning how to effectively utilize various ICT tools and systems for both personal and professional development.

The understanding, management and configuration of the available technology might vary the concept of ICT from a collection of tools and devices used for particular tasks, e.g, publishing, course delivery, and transaction processing. ICT has several definitions depending on the nature of its use, for this text ICT (information and communication technology) is used as an umbrella term that includes any communication devices or applications, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems, as well as the various services and applications associated with them, such as videoconferencing and open and distance learning. ICT have been touted as potentially powerful enabling tools for educational change and reform. When use appropriately different ICTs are said to expend access to education, strengthen the relevance education to the increasingly digital workplace and raise educational quality among others, helping make teaching and learning into an engaging active process connected to real life. It

has been argued that ICT is a principal driver of economic development and social change worldwide (Okwudishu 2014).

2.1.2 Impact of ICT Training on Employees

Information and communication Technology as a significant role in the life of employees. In this aspect, some of the impact are explain below;

2.1.2.1 Knowledge of Accounting Software

ICT training equips employees with skills to use computers, digital tools, and software applications. A key area of this training often includes accounting software (like QuickBooks, Sage, Xero, or SAP), which is vital for financial tasks.

Current professional accountants use a wide range of computer applications to perform their day-to-day operational work (Do et al., 2020; Blankley et al., 2019; Boulianne, 2014). Information communication technology (ICT) has been considered as a major aspect of effective and efficient accounting system and which can leads to increase organizational performance drastically. Information communication technology (ICT) has been used to enhance organizational performance and the reliability of accounting information (Ganyam and Ivungu, 2019).

Accounting information systems include both computer software and hardware which help in recording accounting information (Knapp, 2019) Rapid movement in adoption of information iechnology (IT) by organizations helps to acquire and implement daily

accounting operations using computerized accounting software. Most of the accounting software are user-friendly for accountants, which resulted in functioning of accounting tasks on a daily basis, in a timely manner and accurately. Most of the organizations now replaced their traditional method (manual accounting system) with computerized accounting systems. It is encouraged that continuous effort is required to equip future accountants with necessary IT knowledge and skill as the interconnectedness among IT and accounting functional areas in an organization is invariably important.

2.1.2.2 Enhance Communication and Collaboration

Technology has made communicating with others easier than ever, which is important in today's corporate environment where many organizations are still working from home and face to face interaction is nominal. Cloud based platforms such as Microsoft Teams, Zoom, and others continue to provide a pathway for organizations to remain connected and achieve a level of communication that is arguably better than pre-pandemic and the shift to remote work.

That is largely in part because productivity platforms and applications supply features such as chat, file storage and sharing, and document collaboration to significantly enhance collaboration. What's more, this technology actually increases productivity for an organization and its employees, as feedback on a specific project or task can quickly be sent via instant message, limiting the number of emails and reducing response times.

2.1.2.3 Increase Security

With cyber criminals' attack techniques increasing in volume and complexity, it is of the utmost importance that organizations have sophisticated security measures in place to help prevent infiltration of their network and systems that could lead to a costly data breach or worse. While security technologies like antivirus and multifactor authentication are necessary and effective tools, organizations must also implement controls at the employee level. After all, nearly 9 out of 10 – or 88% – of all data breaches are caused by human error.

As employees are oftentimes the last line of defense in an attempted cyber attack, it is critical to equip them with the knowledge to recognize when such an attack is taking place and what steps they should take to mitigate the threat. This can be achieved through implementing a security awareness training program. These programs aim to educate users on threat vectors and attack techniques and even provide real-world scenarios via simulated campaigns. For employees that are phish prone, additional training can be done to improve their detection skills. This will go a long way in creating a "human firewall" and increasing security for the organization.

2.1.2.4 Improve Productivity and Efficiency

With the use of technology in workplaces, organizations have been able to increase their productivity and efficiency at a rapid pace. Processes that were once manual and time-consuming can now be achieved in a quick and efficient manner with digital tools, applications, and systems. Because of this digital shift, employees have the ability to focus on more important tasks that generate revenue and drive the company forward.

Additionally, leveraging business programs and management software can actually improve the accuracy and effectiveness of departmental functions, as it decreases the likelihood of human error while providing real time data and analytics through dashboards and reporting.

2.1.3 Concept of Accounting Fraud

Accounting fraud refers to the intentional manipulation, misstatement, or falsification of financial records with the aim of deceiving stakeholders, evading tax obligations, misrepresenting a firm's financial position, or gaining unwarranted financial advantage. Such acts may include overstating revenues, understating liabilities, omitting critical transactions, fabricating accounting entries, unauthorized diversion of assets, or presenting distorted financial statements to investors, regulators, and auditors (Bhasin, 2020; Albrecht et al., 2021).

Accounting fraud undermines the core principles of transparency, reliability, and accountability in financial reporting. It can result in significant financial losses, legal penalties, erosion of investor confidence, and reputational damage to an organization (Yadav & Ranjan, 2022). Beyond the immediate monetary implications, fraudulent accounting can also distort market efficiency, mislead financial analysts, and create long-term instability in capital markets (Okoye & Ofoegbu, 2023).

Typically, accounting fraud arises when internal control mechanisms are weak, supervisory oversight is lacking, or employees exploit technical loopholes within computerized accounting systems. In technologically driven accounting environments, fraudsters may manipulate system settings, bypass audit trails, or collude with others to override programmed controls, making detection more difficult (Muneer & Batool, 2021; Otekunrin et al., 2023). As noted by Arora and Mehta (2023), modern

accounting fraud is increasingly sophisticated, often involving the use of technology to conceal illicit financial activities and outmaneuver traditional audit techniques.

Another important dimension of accounting fraud is the behavioral aspect. According to the Fraud Triangle Theory developed by Cressey, fraud is likely to occur when there is pressure (such as financial need), opportunity (such as poor controls), and rationalization (justifying the act) (Cressey, as cited in Bhasin, 2020). Employees or management under pressure, who perceive the opportunity and can justify their actions, are more prone to engage in fraudulent behavior.

Recent high-profile cases both internationally and within Nigeria have reinforced the urgent need for robust anti-fraud mechanisms. For instance, the failure of companies such as Wirecard in Germany and the accounting irregularities reported in some Nigerian financial institutions highlight how accounting fraud continues to pose a serious challenge to financial transparency (Adebisi & Alao, 2021; Ejeh & John, 2022).

In response, many organizations are investing in Information Communication Technology (ICT) tools that support fraud detection and prevention, including forensic accounting systems, real-time financial monitoring, and automated controls. However, the effectiveness of these tools heavily depends on the level of competence and ethical orientation of the employees operating them (Oladejo et al., 2022). Therefore, addressing accounting fraud requires not only technological safeguards but also employee awareness, training, and an organizational culture that promotes accountability and ethical conduct.

2.2 Review of Theories

A sound theoretical framework provides the foundation for understanding the relationship between ICT training and accounting fraud prevention. This study adopts two major theories: the Fraud Triangle Theory and the Technology Acceptance Model (TAM). These theories help explain both the behavioral and technological dimensions of fraud risk and control within organizations.

2.2.1 Fraud Triangle Theory

The Fraud Triangle Theory, developed by Donald Cressey in the 1950s, remains one of the most widely cited frameworks in fraud studies. It identifies three key elements that must be present for occupational fraud to occur: *pressure*, *opportunity*, and *rationalization* (Bhasin, 2020).

- Pressure refers to the motivation or financial need driving the individual to commit fraud.
- Opportunity is the perceived ability to commit fraud without being caught.
- Rationalization involves the internal justification for unethical behavior.

In the context of ICT systems, opportunity often emerges when employees lack the knowledge or training to use or secure digital tools appropriately. Poorly trained employees may unintentionally leave systems vulnerable to breaches or misuse. They may also exploit their lack of oversight or inadequate ICT controls to perpetrate fraud (Yadav & Ranjan, 2022). ICT training directly addresses this opportunity component by equipping employees with the knowledge to adhere to internal controls, recognize system vulnerabilities, and understand the consequences of data manipulation. When employees are well-trained in using accounting software, ERP systems, and cybersecurity protocols, the scope for committing fraud is significantly reduced (Teixeira & Souza, 2020). Trained users are also more capable of identifying

irregularities and reporting them early, enhancing the overall fraud detection capability of the organization.

Thus, the Fraud Triangle Theory underlines the preventive power of ICT training in reducing the opportunity for fraudulent behaviour within digital accounting environments.

2.2.2 Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM), introduced by Davis in 1989, is a behavioural theory that explains how users come to accept and use technology. According to TAM, two major factors influence the acceptance of technology:

- Perceived Usefulness (PU) – the degree to which a person believes that using a particular system would enhance job performance.
- Perceived Ease of Use (PEOU) – the degree to which a person believes that using a system would be free of effort (Davis, as cited in Adebisi & Alao, 2021).

ICT training plays a critical role in improving both perceived usefulness and ease of use. When employees receive systematic training, they gain confidence in operating accounting systems, understanding features like fraud alerts, access control, audit trails, and real-time monitoring tools. This makes them more likely to use such systems effectively and consistently (Oladejo et al., 2022).

Moreover, training reduces user resistance to adopting new or upgraded fraud detection systems, thereby enhancing the organization's capacity to prevent accounting fraud. Employees who perceive technology as easy and beneficial are

more engaged in maintaining data accuracy, monitoring transactions, and complying with fraud prevention protocols (Nguyen & Huynh, 2021).

By applying TAM, this study emphasizes that ICT training does not only improve technical competence but also promotes favorable attitudes toward fraud prevention technologies. This makes the model highly relevant in explaining the behavioral change that training induces among accounting personnel.

2.3 Empirical Review

This section discusses empirical findings relating to each variable in the study — focusing on employee ICT training, accounting software usage, cybersecurity measures and automated internal control as the independent variable and accounting fraud prevention as the dependent variable.

2.3.1 Employee ICT Training and Accounting Fraud Prevention

Teixeira and Souza (2020) carried out a cross-sectional study in Brazil focusing on the role of ICT training in fraud prevention among financial professionals. The study covered 42 financial institutions and employed a quantitative survey design using structured questionnaires administered to accounting and IT personnel. Their findings indicated that organizations that conducted regular and role-specific ICT training experienced significantly fewer internal fraud cases. Employees who received training showed higher competence in using fraud detection software and were more proactive in flagging irregular financial transactions. The authors recommended that ICT training be institutionalized as a core part of internal control policy to strengthen fraud prevention strategies.

Oladejo, Olanrewaju, and Ojo (2022) investigated the impact of ICT literacy on fraud detection across 60 financial firms in Nigeria. Using a mixed-method approach involving both interviews and statistical analysis of survey data, the study found a strong positive correlation between ICT training and reduced fraud occurrences. Employees with structured training were more effective at interpreting fraud alerts and more likely to report suspicious activities. The researchers concluded that regular ICT training fosters better system usage and ethical behavior, thereby lowering fraud risk. They recommended that firms implement quarterly ICT refresher courses, especially in high-risk departments.

Muneer and Batool (2021), in a study conducted across 35 public and private sector organizations in Pakistan, examined the role of ICT training in enhancing fraud reporting culture. The researchers used regression analysis to assess responses from 210 accounting staff. The findings revealed that staff with limited ICT skills were more prone to committing or ignoring fraud, while trained staff were more confident and ethical in their handling of financial records. They advised that organizations prioritize employee competence development, particularly in accounting software and internal audit systems.

Adebisi and Alao (2021) conducted a study in Nigeria involving 48 firms in the manufacturing and service sectors. The researchers used structured questionnaires and applied correlation analysis to determine the influence of ICT training on accounting transparency. The study revealed that trained employees were more compliant with financial regulations and frequently used system features such as audit trails and data backup tools. This improved accountability and reduced fraud incidents. They recommended policy-driven ICT onboarding programs for all financial staff.

Singh and Verma (2020) analyzed cybersecurity practices in 30 Indian enterprises, focusing on how employee ICT training influenced the rate of financial fraud. Using content analysis of fraud reports and staff training records, the study found that lack of training on system use and data security was a major factor behind unauthorized access and data breaches. They emphasized the importance of cybersecurity training as a core component of fraud prevention and suggested monthly ICT drills to simulate real-time threats.

In a study conducted by Arora and Mehta (2023) across 22 fintech firms in India, the researchers applied a case study methodology to examine how digital literacy affected fraud risk. The firms selected had previously reported fraud incidents. The findings highlighted that most fraud cases occurred where employees had minimal understanding of system protocols or failed to follow standard operating procedures. The authors recommended that firms use gamified learning platforms to improve ICT awareness among employees and track training progress.

Yadav and Ranjan (2022) examined the effectiveness of ICT-based training on fraud reduction across 50 financial institutions in Bangladesh. Using a quasi-experimental design, the researchers split staff into a control group and a training group. After six months, the trained group recorded 36% fewer fraud incidents compared to the control group. Their findings suggest that timely and relevant ICT training can significantly strengthen fraud detection. They recommended continuous training assessment and technology-specific skill upgrades.

Nguyen and Huynh (2021) explored the link between cybersecurity awareness training and fraud reduction in 40 Vietnamese banks. The researchers adopted a qualitative research design through focus group discussions and interviews with IT

and accounting staff. Their study revealed that trained employees were more conscious of phishing scams, social engineering tactics, and password protocols. These employees also demonstrated better understanding of fraud red flags, leading to quicker response times. The study suggested implementing ICT certification requirements for financial staff.

Okoye and Ofoegbu (2023) assessed the effectiveness of digital competency training in reducing accounting fraud among 38 private firms in Lagos, Nigeria. The researchers used descriptive statistics and ANOVA to analyze data collected from 190 respondents. Their results indicated that firms with structured ICT training programs had lower incidences of financial misstatement and asset misappropriation. They recommended that internal audit units collaborate with HR departments to schedule periodic digital skills workshops.

Lastly, Bello and Yusuf (2024) conducted a longitudinal study involving 25 firms in Ghana's telecommunications and finance sectors. Over a 12-month period, they tracked the impact of employee ICT training on fraud occurrence using time-series analysis. The study revealed a gradual decline in fraud cases in firms that embedded ICT training into their onboarding and compliance processes. Findings showed a 25% reduction in recorded frauds compared to firms without such training programs. They advocated for integrating ICT modules into corporate governance policies.

2.3.2 Accounting Software Usage and Accounting Fraud Prevention

Accounting software manages and records the day-to-day financial transactions of an organization, including fixed asset management, expense management, revenue management, accounts receivable, accounts payable, subledger accounting, and reporting and analytics. A complete accounting system keeps track of an

organization's assets, liabilities, revenues, and expenses. These transactions then populate the general ledger in real time, providing CFOs, treasurers, and controllers immediate access to real time, accurate financial data. It also allows P&L owners visibility into their performance at the operational level.

The systematic recording of these financial transactions enables the production of quarterly and annual financial statements, including balance sheets, income statements, statements of cash flows, and statements of stockholders' equity. Accounting software is a key component of an enterprise resource planning (ERP) system.

ERP systems unify essential business functions, such as accounting, financial planning and analysis (FP&A), supply chain, inventory management, and procurement. These applications are natively integrated with a common user interface and data model, eliminating the need to move between systems or integrate siloed data to manage different aspects of your business.

Thottoli (2020) noted that the introduction of accounting software brought changes to financial accounting process (data entry, storage and financial statement preparation); as well as internal control. While the aforementioned can be viewed as having positive impact on banking operations, there are obvious pitfalls and challenges that could arise from it, including the financial impact of such pitfalls on the organization (Turner et al., 2020). The replacement of manual accounting system by computer-based brings about risk of on-line fraud (Arnestesa, 2018). There are also complexities in familiarization with the system, system failure and error or fraud that could accompany its implementation. The Chartered Institute of Public Finance and Accountancy, United Kingdom defined fraud as an intentional distortion of financial

statement or otherwise, for personal benefit. The International Auditing Guidelines (IAG) defines fraud as a type of irregularity, involving the use of deceits to obtain an illegal or unjust advantage, which involves alteration, manipulation or falsification of figures or documents.

Fraud has eaten deep into private organizations in Nigeria in spite of numerous regulations put in place by government to avert the occurrence of fraud being perpetuated by the bank staff. It is unarguable to say fraud is an epidemic in Nigeria (Olaoye & Dada, 2014). Oseni (2006) cited in Olaoye and Dada (2014) argued that continuous perpetuation of frauds in Nigerian private sector organizations has casted doubt in the mind of the stakeholders in the industry regarding reliability of banks audited accounts. Whereas, Oseni and Idolo (2010) stressed that the spate of fraudulent activities in private industry in Nigeria has prompted law enforcement agencies to declare war against fraud perpetrators to stop the industry from being source of embarrassment to the country.

2.3.3 Enterprise Resource Planning (ERP) and Accounting Fraud Prevention

Enterprise resource planning (ERP) is the integrated management of main business processes, often in real time and mediated by software and technology. ERP is usually referred to as a category of business management software typically a suite of integrated applications that an organization can use to collect, store, manage and interpret data from many business activities. ERP systems can be local-based or cloud-based. Cloud-based applications have grown in recent years due to the increased efficiencies arising from information being readily available from any location with Internet access. ERP differs from integrated business management systems by including planning all resources that are required in the future to meet

business objectives. This includes plans for getting suitable staff and manufacturing capabilities for future needs.

ERP provides an integrated and continuously updated view of the core business processes using common databases maintained by a database management system. ERP systems track business resources—cash, raw materials, production capacity and the status of business commitments: orders, purchase orders, and payroll. The applications that make up the system share data across various departments (manufacturing, purchasing, sales, accounting, etc.) that provide the data. Almajali, Dmaithan (2016), ERP facilitates information flow between all business functions and manages connections to outside stakeholders (Radovilsky, Zinovy, 2004)

According to Gartner, the global ERP market size is estimated at $35 billion in 2021. Though early ERP systems focused on large enterprises, smaller enterprises increasingly use ERP systems. The ERP system integrates varied organizational systems and facilitates error-free transactions and production, thereby enhancing the organization's efficiency. However, developing an ERP system differs from traditional system development. Shaul, L.; Tauber, D. (2012) ERP systems run on a variety of computer hardware and network configurations, typically using a database as an information repository.

While prevention is the primary goal, no system is completely fraud-proof. This is where ERP’s reporting and analysis capabilities become crucial. The comprehensive data collection within ERP systems creates a rich source for forensic accounting if fraud is suspected. Detailed audit logs show exactly who accessed what information and when, making it easier to investigate suspicious activity. Historical transaction data allows for pattern analysis to identify when fraudulent behavior began and its full

extent. This information proves invaluable not only for internal investigation but also for law enforcement and legal proceedings if necessary.

The reporting capabilities also support regular compliance activities and external audits. Rather than scrambling to compile information for auditors, companies with robust ERP systems can quickly generate the reports and transaction details needed, demonstrating their commitment to transparency and proper controls.

While ERP offers powerful tools for fraud prevention, implementation requires careful planning to maximize these benefits. Simply installing the software isn't enough companies must configure the system to match their specific control needs and risk profile.

Start by mapping existing business processes and identifying potential fraud vulnerabilities. This assessment should guide configuration decisions, particularly around approval workflows and access controls. Too many organizations implement ERP with minimal customization of security settings, undermining the system's fraud prevention potential. User training represents another critical success factor. Even the best system controls can be circumvented if users share login credentials, leave workstations unlocked, or find workarounds for processes they find cumbersome. Effective training should emphasize not just how to use the system but why specific controls matter for organizational integrity.

Finally, regular system reviews ensure that ERP controls continue to match evolving business needs. As organizations grow, add new business lines, or change processes, they must update system configurations to maintain strong fraud prevention capabilities.

2.3.4 Cybersecurity and Accounting fraud

The growing incorporation of digital technologies in accounting has required a strong emphasis on cybersecurity to safeguard sensitive financial information. A substantial body of literature has developed examining diverse facets of cybersecurity within the accounting profession, underscoring its vital significance. Cybersecurity threats present considerable dangers to the accounting sector. A thorough analysis by the Ponemon Institute (2020) indicates that financial data breaches are among the most expensive and prevalent, with the average cost of a breach in the financial sector markedly exceeding that of other industries. This highlights the susceptibility of financial data to cyberattacks and the significant financial repercussions of such breaches. Numerous studies have investigated the application of cybersecurity protocols in accounting. Iyana Kumar (2023) underscores the necessity of a multi-faceted security strategy, incorporating firewalls, intrusion detection systems, and encryption, to safeguard financial data. The research highlights the significance of cybersecurity policies and ongoing employee training in reducing cyber threats. Atreyi Kankanhalli, (2003) examine the incorporation of security protocols into organizational processes and emphasize the necessity for ongoing surveillance and enhancement of these protocols to counteract emerging threats.

The impact of technological advancements on improving cybersecurity in accounting has been thoroughly examined. John Williams Rittinghouse and James Ransome (2017) examine how cloud computing, despite providing scalability and efficiency, also presents novel security challenges. They promote sophisticated encryption and secure access protocols to protect cloud-stored financial information. Kim-Kwang Raymond Choo (2016) examines the application of artificial intelligence (AI) and machine learning (ML) in cybersecurity, emphasizing their capacity to identify

anomalies and thwart cyberattacks in real-time. Regulatory frameworks are essential in influencing cybersecurity practices within the accounting sector. The American Institute of Certified Public Accountants offers directives on cybersecurity risk management, highlighting the necessity for accounting firms to adhere to regulatory mandates for data protection. Research conducted by the Securities and Exchange Commission (SEC) underscores the necessity of compliance with regulations such as the General Data Protection Regulation (GDPR) and the Sarbanes-Oxley Act (SOX), which impose rigorous cybersecurity protocols to safeguard financial data David Tersteeg (2018).

Notwithstanding the progress in cybersecurity technologies, numerous challenges remain in their application within the accounting profession. Elvis Brynjolfsson (2017) address the significant expenses and intricacies associated with implementing extensive cybersecurity protocols, which can be especially onerous for small and medium-sized accounting firms. The deficit of proficient cybersecurity experts presents a considerable challenge, as noted by Alan Smith and Williams Rupp (2002), who contend that ongoing education and training are crucial for preparing accounting professionals to adeptly address cybersecurity threats. The ethical ramifications of cybersecurity in accounting represent a significant area of concern. Research has emphasized concerns regarding data privacy and the ethical application of cybersecurity instruments. Sarah Al-Mansoori and Mohammed Ben Salem (2023) examine the ethical implications of employing AI in cybersecurity, highlighting the importance of transparency and accountability in the implementation of these technologies.

The growing incorporation of digital technologies in accounting has required a strong emphasis on cybersecurity to safeguard sensitive financial information. A substantial

body of literature has developed examining diverse facets of cybersecurity within the accounting profession, underscoring its vital significance. Cybersecurity threats present considerable dangers to the accounting sector. A thorough analysis by the Ponemon Institute (2020) indicates that financial data breaches are among the most expensive and prevalent, with the average cost of a breach in the financial sector markedly exceeding that of other industries. This highlights the susceptibility of financial data to cyberattacks and the significant financial repercussions of such breaches.

Numerous studies have investigated the application of cybersecurity protocols in accounting. Iyana Kumar (2023) underscores the necessity of a multi-faceted security strategy, incorporating firewalls, intrusion detection systems, and encryption, to safeguard financial data. The research highlights the significance of cybersecurity policies and ongoing employee training in reducing cyber threats. Atreyi Kankanhalli (2003) examine the incorporation of security protocols into organizational processes and emphasize the necessity for ongoing surveillance and enhancement of these protocols to counteract emerging threats. The impact of technological advancements on improving cybersecurity in accounting has been thoroughly examined. Kim-Kwang Raymond Choo (2011) examines the application of artificial intelligence (AI) and machine learning (ML) in cybersecurity, emphasizing their capacity to identify anomalies and thwart cyberattacks in real-time. Regulatory frameworks are essential in influencing cybersecurity practices within the accounting sector. The American Institute of Certified Public Accountants offers directives on cybersecurity risk management, highlighting the necessity for accounting firms to adhere to regulatory mandates for data protection AICPA-CIMA (2023). Research conducted by the Securities and Exchange Commission (SEC) underscores the necessity of compliance

with regulations such as the General Data Protection Regulation (GDPR) and the Sarbanes-Oxley Act (SOX), which impose rigorous cybersecurity protocols to safeguard financial data. Notwithstanding the progress in cybersecurity technologies, numerous challenges remain in their application within the accounting profession. Elvis Brynjolfsson (2023) address the significant expenses and intricacies associated with implementing extensive cybersecurity protocols, which can be especially onerous for small and medium-sized accounting firms.

2.3.5 Automated Internal Controls in Preventing Accounting Fraud

Internal control mechanisms are essential frameworks implemented by organizations to ensure efficient operations, reliable financial reporting, and compliance with regulations (Kaawaase et al., 2021). These mechanisms consist of various components and types aimed at safeguarding assets, preventing fraud, and promoting operational effectiveness. Control Environment, this component sets the tone of an organization, influencing the control consciousness of its employees. It includes the integrity and ethical values of management, as well as the organization's commitment to competence and accountability (Wangloan et al., 2022). Risk Assessment, organizations must identify and analyze risks that could hinder the achievement of objectives. Risk assessment involves evaluating potential risks, their likelihood, and potential impact on the organization's goals and operations. Control Activities, these are the policies and procedures that help ensure management directives are carried out. Control activities can include approvals, authorizations, verifications, reconciliations, and segregation of duties to prevent errors and fraud (Danter, 2022, Antwi et al., 2024, Bello et al., 2023a). Information and Communication, effective internal controls require timely, relevant, and reliable communication of information (Lois et al., 2020). This component ensures that information flows internally, providing necessary data to

enable people to carry out their responsibilities. Monitoring Activities, continuous monitoring of controls is essential to assess their effectiveness over time. Monitoring involves ongoing assessments, evaluations, and reporting of internal control processes, identifying deficiencies, and implementing necessary improvements (Turetken et al., 2020).

Internal controls are categorized into three main types based on their purpose and function (Li et al., 2020). Preventive Controls, these controls are designed to prevent errors or irregularities before they occur (Lartey et al., 2020, Eziefule et al., 2022). Examples include segregation of duties, proper authorization procedures, physical access restrictions, and employee training on policies and procedures. Preventive controls aim to establish barriers that deter potential issues from arising. Detective Controls, detective controls are implemented to identify errors or irregularities after they have occurred, examples include reconciliations, regular reviews and comparisons of data, performance evaluations, and audits (Al-Zoubi, 2021; Naboth-Odums et al., 2021). Detective controls help detect deviations from expected outcomes and facilitate timely corrective actions. Corrective Controls, once errors or irregularities are identified, corrective controls are implemented to mitigate their impact and prevent recurrence. Corrective actions may involve adjustments to processes, policies, or procedures to address root causes and strengthen internal controls (Abiodun, 2020). Examples include disciplinary actions, process redesign, and enhanced training programs.

Fraud prevention is a critical aspect of organizational governance, aimed at minimizing the risk of fraudulent activities that can lead to financial losses, reputational damage, and legal repercussions (Taherdoost, 2021; Rashid, 2022). Effective fraud prevention strategies rely on robust internal controls, including

preventive measures, vigilant monitoring, and proactive risk management practices. Preventive controls are foundational in fraud prevention, focusing on establishing barriers and safeguards to deter fraudulent activities before they occur. Key preventive controls include. Segregation of Duties, this control principle ensures that no single individual has control over all key aspects of a transaction or financial process (Rauterberg, 2021). By separating responsibilities among different individuals, organizations reduce the risk of collusion and unauthorized activities. For example, separating the roles of initiating transactions, recording transactions, and authorizing payments enhances accountability and oversight. Authorization and Approval Processes, strict authorization and approval procedures require designated personnel to authorize transactions or access based on predefined criteria and limits (Khan et al., 2022). These processes ensure that transactions are legitimate and comply with organizational policies and regulatory requirements. Proper authorization mitigates the risk of unauthorized transactions and ensures accountability throughout the transaction lifecycle. Physical and Logical Access Control, physical access controls restrict physical access to sensitive areas, assets, or information through measures such as locks, security guards, and surveillance systems (Masoumzadeh et al., 2022).

Logical access controls, on the other hand, regulate access to computer systems, networks, and data through authentication mechanisms, passwords, and user permissions. These controls prevent unauthorized access to critical assets and sensitive information, reducing the likelihood of fraudulent activities (Saxena et al., 2020). Several organizations have successfully implemented preventive controls to mitigate fraud risks (Saxena et al., 2020). For instance, a multinational corporation implemented stringent segregation of duties across its financial operations, ensuring that no single employee could initiate, approve, and process payments without

oversight. This measure significantly reduced the potential for fraudulent payments and unauthorized transactions. In another example, a financial institution enhanced its authorization and approval processes for high-value transactions by implementing dual authorization requirements and strict verification procedures. This proactive approach prevented fraudulent fund transfers and strengthened the institution's fraud prevention framework (Barker, 2020).

Despite the benefits of preventive controls, organizations face several challenges and limitations in effectively preventing fraud. Implementing and maintaining robust preventive controls can be resource-intensive, requiring investments in technology, training, and ongoing monitoring (Bandari, 2021). Small and medium-sized enterprises (SMEs) may encounter challenges due to limited budgets and capabilities. Fraudsters continually evolve their tactics, making it challenging for organizations to anticipate and address emerging fraud schemes effectively (Rossy and Ribaux, 2020). Preventive controls must be adaptable and responsive to evolving fraud risks and technological advancements. Ensuring employee awareness of fraud risks and adherence to control procedures is crucial. Lack of training, understanding, or compliance with control measures can undermine the effectiveness of preventive controls. Stringent preventive controls may sometimes impede operational efficiency or agility, particularly in dynamic business environments (Plant et al., 2022). Organizations must strike a balance between fraud prevention and maintaining efficient business processes. Effective fraud prevention requires a holistic approach that integrates preventive controls, proactive monitoring, and continuous improvement efforts (Musyoki, 2023). By implementing robust segregation of duties, rigorous authorization processes, and comprehensive access controls, organizations can strengthen their defenses against fraud.

2.3.6 ICT Training and Fraud Prevention

ICT training plays a pivotal role in the prevention and detection of accounting fraud by equipping employees with the skills and awareness necessary to identify, resist, and mitigate fraudulent activities within technology-driven accounting systems. In today's increasingly digital work environment, financial fraud is no longer limited to traditional paper-based manipulation. It now often involves sophisticated exploitation of computerized accounting systems, data breaches, unauthorized access, and manipulation of electronic financial records. Consequently, employee ICT training has become a critical tool in strengthening an organization's fraud control mechanisms (Teixeira & Souza, 2020; Singh & Verma, 2020).

When employees are trained in ICT, they gain the ability to properly utilize fraud-prevention features embedded in accounting systems. These include the effective use of audit trails, which provide transparent and chronological records of all transactions and system activities; role-based access controls, which limit data access to authorized personnel only; strong password protocols and encryption, which prevent unauthorized access to sensitive financial data; and internal audit controls, which help in early detection of anomalies (Nguyen & Huynh, 2021). Through ICT training, employees are taught how these features work and how to apply them appropriately to prevent manipulation of financial data.

Furthermore, training reduces the risk of human error or negligence—both of which are common causes of fraud vulnerabilities. Employees who lack digital skills may inadvertently disable system controls, ignore warning messages, or fall victim to phishing scams and other cyber threats (Oladejo et al., 2022). In contrast, trained personnel are more vigilant, capable of identifying suspicious behavior, and proactive

in safeguarding the organization's accounting infrastructure. As noted by Arora and Mehta (2023), trained employees are less susceptible to social engineering attacks and more capable of responding appropriately to fraud risks when they arise.

In addition to technical competence, ICT training fosters an ethical culture of accountability and transparency. Employees who understand how systems function and the consequences of bypassing controls are more likely to adhere to ethical standards and organizational policies. Moreover, such training often includes guidance on reporting procedures, whistleblowing mechanisms, and fraud red flag indicators. Employees who are confident in their ICT skills are more willing to report suspicious activities, thereby strengthening the organization's internal oversight and fraud detection capabilities (Yadav & Ranjan, 2022).

Importantly, continuous ICT training keeps employees updated on evolving cyber risks, new fraud schemes, and technological updates. This is particularly critical in environments where cybercriminals constantly develop more advanced tactics to exploit system weaknesses. Organizations that implement regular ICT training sessions not only build employee competence but also improve overall system resilience to fraud (Adebisi & Alao, 2021).

In summary, ICT training contributes directly to fraud prevention by enhancing employees' technical capacity, ethical orientation, and fraud detection capabilities. It empowers them to use system features effectively, recognize vulnerabilities, and take preventive measures that uphold the integrity of financial reporting.

REFERENCES

Alan D. Smith and William T. Rupp(2022). Issues in Cybersecurity: Understanding the Potential Risks Associated with Hackers/Crackers, Information Management & Computer Security, vol. 10, no. 4, pp. 178–183. DOI: 10.1108/09685220210436969.

Atreyi Kankanhalli, Hock-Hal Teo, Bernard. C. Y. Tan, and Kwok-Keewei (2023). An integrative study of information systems security effectiveness. International Journal of Information Management, vol. 23, no. 2, pp. 139-154. DOI: 10.1016/S0268-4012(02)00073-4.

Abiodun, E.A. (2020). Internal control procedures and firm's performance. International Journal of Scientific & Technology Research, 9(2), 6407-6415.

Adebisi, J. F., & Alao, T. A. (2021). The impact of technology on financial reporting: A case study approach. International Journal of Finance and Accounting, 12(4), 27–36.

AICPA-CIMA, "The crucial role of cybersecurity for accounting firms," 2023. [Online]. Available: https://www.aicpa-cima.com/professional-insights/article/the-crucial-role-ofcybersecurity-for-accounting-firms

Almajali, Dmaithan (2016). "Antecedents of ERP systems implementation success: a study on Jordanian healthcare sector". Journal of Enterprise Information Management. **29** (4): 549–565. doi:10.1108/JEIM-03-2015-0024.

Al-Zoubi, A.M. (2021). A proposed framework for classifying preventive and detective fraud controls. International Journal of Entrepreneurship, 25, 1-21.

Arora Mehta (2023), modern accounting fraud is increasingly sophisticated, often involving the use of technology to conceal illicit financial activities and outmaneuver traditional audit techniques. General Journal 12(2).

Barker, R. (2020). The use of proactive communication through knowledge management to create awareness and educate clients on e-banking fraud prevention. South African Journal of Business Management, 51(1), 1-10.

Bhasin, M. L. (2020). Fraud in financial reporting: Types, causes, and prevention. Global Journal of Management and Business Research, 20(6), 45–58.

Boulianne (2014), Information Communication Technology program

David Tersteeg(2018). Legislative and Regulatory Obligations on Corporate Attorneys: Production Data in the World of Sarbanes Oxley and General Data Protection, Northern Illinois University Law Review, vol. 39, pp. 456.

Danter, E. (2022). Separation of duties. in audit defense: a management audit readiness guide (pp. 171-205). Cham: Springer International Publishing.

Eziefule, A.O., Adelakun, B.O., Okoye, I.N., & Attieku, J.S. (2022). The role of AI in automating routine accounting tasks: efficiency gains and workforce implications. European Journal of Accounting, Auditing and Finance Research, 10(12), 109-134

Ganyam & Iyungu (2019), Information communication technology (ICT) has been used to enhance organizational performance and the reliability of accounting information. African Journal.

Iyana Kumar(2023). Emerging Threats in Cybersecurity: A Review Article, International Journal of Applied and Natural Sciences, vol. 1, no. 1, pp. 1–8.

John Williams Rittinghouse and James Ransome(2017). Cloud Computing: Implementation, Management, and Security. CRC Press.

Kim-Kwang Raymond Choo(2011). The cyber threat landscape: Challenges and future research directions," Computers & Security, vol. 30, no. 8, pp. 719–731. DOI: 10.1016/j.cose.2011.08.002

Kaawaase, T.K., Nairuba, C., Akankunda, B., & Bananuka, J. (2021). Corporate governance, internal audit quality and financial reporting quality of financial institutions. Asian Journal of Accounting Research, 6(3), 348-366.

Khan, A., Ahmad, A., Ahmed, M., Sessa, J., & Anisetti, M. (2022). Authorization schemes for internet of things: requirements, weaknesses, future challenges and trends. Complex & Intelligent Systems, 8(5), 3919-3941.

Knapp 2019, Accounting Information System. A Nigerian perspective. African Journal of Accounting and Finance, 11(1), 48–64.

Lartey, P.Y., Kong, Y., Bah, F.B.M., Santosh, R.J., & Gumah, I.A. (2020). Determinants of internal control compliance in public organizations; using preventive, detective, corrective and directive controls. International Journal of Public Administration, 43(8), 711-723.

Li, Y., Li, X., Xiang, E., & Djajadikerta, H.G. (2020). Financial distress, internal control, and earnings management: Evidence from China. Journal of Contemporary Accounting & Economics, 16(3), 100210.

Lois, P., Drogalas, G., Karagiorgos, A., & Tsikalakis, K. (2020). Internal audits in the digital era: opportunities risks and challenges. EuroMed Journal of Business, 15(2), 205- 217.

Masoumzadeh, A., van der Laan, H., & Dercksen, A. (2022, June). BlueSky: physical access control: characteristics, challenges, and research opportunities. In Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies (pp. 163-172)

Muneer, S., & Batool, S. (2021). Role of ICT in corporate governance: A case study on financial transparency. Business & Economic Review, 16(3), 61–74.

Musyoki, K.M. (2023). Internal control systems and their role in financial fraud prevention in Kenya. African Journal of Commercial Studies, 3(3), 173-180

Naboth-Odums, A., Abanyam, F.E., Edeh, N.I., & Abdulkadir, A. (2021). Procedural preventive and detective control measures adopted by

administrative officers for effective information management in Colleges of Education in South-South.

Nguyen, T. D., & Huynh, H. T. (2021). The role of cybersecurity measures in fraud prevention: A case study of financial institutions. International Journal of Financial Security, 9(1), 14-22.

Okoye, E., & Ofoegbu, G. (2023). Corporate fraud and investor confidence in emerging markets: A Nigerian perspective. African Journal of Accounting and Finance, 11(1), 48–64.

Okoye, E., & Ofoegbu, G. (2023). Corporate fraud and investor confidence in emerging markets: A Nigerian perspective. African Journal of Accounting and Finance, 11(1), 48–64.

Oladejo, M. O., Olanrewaju, M. O., & Ojo, A. O. (2022). Impact of ICT on fraud detection in financial organizations. International Journal of Accounting and Finance, 13(2), 102–118.

Plant, O.H., van Hillegersberg, J., & Aldea, A. (2022). Rethinking IT governance: Designing a framework for mitigating risk and fostering internal control in a DevOps environment. International Journal of Accounting Information Systems, 45, 100560.

Ponemon Institute, Cost of a Data Breach Report 2020.

Radovilsky, Zinovy (2004). Bidgoli, Hossein (ed.). The Internet Encyclopedia, Volume 1. John Wiley & Sons, Inc. p. 707. ISBN 9780471222026.

Rauterberg, G. (2021). The separation of voting and control: the role of contract in corporate governance.

Rossy, Q., & Ribaux, O. (2020). Orienting the development of crime analysis processes in police organisations covering the digital transformations of fraud mechanisms. European Journal on Criminal Policy and Research, 26, 335-356.

Sarah Al-Mansoori and Mohammed Ben Salem(2023). The role of artificial intelligence and machine learning in shaping the future of cybersecurity: trends, applications, and ethical considerations, International Journal of Social Analytics, vol. 8, no. 9, pp. 1–16, 2023.

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.K.R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. Electronics, 9(9), 1460.

Shaul, L.; Tauber, D. (2012). "CSFs along ERP life-cycle in SMEs: a field study". Industrial Management & Data Systems. **112** (3): 360–384. doi:10.1108/02635571211210031.

Singh, R., & Verma, S. (2020). The impact of technology on fraud detection and prevention: A comparative study of ICT systems. International Journal of Information Security, 17(6), 301–314.

Taherdoost, H. (2021). A review on risk management in information systems: Risk policy, control and fraud detection. Electronics, 10(24), 3065.

Teixeira, L., & Souza, M. (2020). The role of employee ICT training in fraud prevention. Journal of Organizational Behaviour, 35(4), 217–230.

Turetken, O., Jethefer, S., & Ozkan, B. (2020). Internal audit effectiveness: operationalization and influencing factors. Managerial Auditing Journal, 35(2), 238-271.

Wangloan, E.H., Moeins, A., Marhalinda, M., & Endri, E. (2022). The influence of transformational leadership, professional ethics, and work competence on organizational commitment and its implications for the performance of ship safety.

Yadav, R., & Ranjan, P. (2022). Corporate accounting fraud: Causes, detection and prevention. International Journal of Corporate Governance, 7(3), 214–228.

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This chapter describes the methodology employed in carrying out the study. It presents the research design, target population, sample size determination, sampling technique, methods of data collection, model specification, operationalization of variables, methods of data analysis, and ethical considerations.

3.2 Research Design

The study adopted a descriptive survey research design. This design was considered appropriate because the study sought to describe the relationship between Information and Communication Technology (ICT) practices and accounting fraud prevention. Descriptive design is suitable when variables have already occurred and are beyond the control of the researcher (Mugenda & Mugenda, 2003). Moreover, it allows for collection of primary data from a relatively large population for the purpose of generalization (Cohen, Manion & Morrison, 2000).

3.3 Population of the Study

The target population of this study comprised **700 private firms in Benin City**. These firms were chosen because they rely heavily on ICT systems in accounting processes, making them suitable for investigating the influence of ICT on accounting fraud prevention.

3.4 Sample Size Determination

The sample size was determined using the Taro Yamane (1967) formula:

$n = N / (1 + N(e^2))$

Where:

- n = sample size
- N = population size (700)
- e = level of precision (0.05 at 95% confidence level)

Substituting the values:

$n = 700 / (1 + 700(0.05^2))$

$n = 700 / (1 + 700(0.0025))$

$n = 700 / (1 + 1.75)$

$n = 700 / 2.75$

$n \approx 255$

Thus, the sample size for this study is 255 respondents drawn from private firms in Benin City.

3.5 Sampling Technique

The study employed a convenience sampling technique due to the practical challenges of reaching all firms in the city. This technique ensured that respondents who were readily available and knowledgeable about ICT practices and accounting fraud prevention were included.

3.6 Method of Data Collection

Data were collected using **structured questionnaires** complemented by interviews. The questionnaire contained both closed and open-ended questions designed to capture information on ICT variables such as accounting software usage, cybersecurity measures, automated internal controls, and ICT training, as well as their influence on accounting fraud prevention. Interviews were also conducted with selected managers to provide deeper insights and triangulate responses.

3.7 Model Specification

The study adopted a multiple regression model to test the relationship between ICT variables and accounting fraud prevention. The model is expressed as:

$$AFP = \beta 0 + \beta 1ASU + \beta 2CSM + \beta 3AIC + \beta 4ICTT + \mu$$

Where:

- AFP = Accounting Fraud Prevention (dependent variable)
- ASU = Accounting Software Usage
- CSM = Cybersecurity Measures
- AIC = Automated Internal Controls
- ICTT = Employee ICT Training
- $\beta 0$ = Intercept
- $\beta 1 - \beta 4$ = Coefficients of the independent variables
- μ = Error term

3.8 Operationalization of Variables

Variable	Type	Indicators	Measurement Scale	Expected Relationship
Accounting Fraud Prevention (AFP)	Dependent	Frequency of fraud cases, detection rate, prevention mechanisms	Ordinal	-
Accounting Software Usage (ASU)	Independent	Extent of software adoption, efficiency of usage, accuracy of reporting	Likert scale	Positive
Cybersecurity Measures (CSM)	Independent	Encryption, multi-factor authentication, firewalls	Likert scale	Positive
Automated Internal Controls (AIC)	Independent	Use of audit trails, error detection, system alerts	Likert scale	Positive
Employee ICT Training (ICTT)	Independent	Frequency of training, quality of training programs, staff competence	Likert scale	Positive

Author compilation 2025

3.9 Method of Data Analysis

Data collected from the questionnaires were coded and analyzed using **descriptive statistics** (mean, frequency, percentages) and **inferential statistics** (multiple regression analysis) with the aid of SPSS/EViews. Descriptive statistics helped to summarize the responses, while regression analysis tested the hypotheses and determined the influence of ICT variables on accounting fraud prevention.

CHAPTER FOUR

DATA PRESENTATION AND ANALYSIS

4.1 Introduction

This chapter presents and analyzes the data collected in line with the objectives and research methodology outlined in Chapter Three. The study examined the influence of Information and Communication Technology (ICT) practices on accounting fraud prevention among private firms in Benin City. Specifically, the study focused on the role of Accounting Software Usage (ASU), Cybersecurity Measures (CSM),

Automated Internal Controls (AIC), and Employee ICT Training (ICTT) on Accounting Fraud Prevention (AFP).

A total of 255 structured questionnaires were administered to managers, accountants, and ICT officers of selected private firms within Benin City. Out of these, 240 questionnaires were properly filled , representing a 94% response rate. The data were analyzed using both descriptive and inferential statistical tools with the aid of the Statistical Package for the Social Sciences (SPSS, version 25) . Descriptive statistics such as frequency, mean, and standard deviation were used to summarize respondents' demographic characteristics and their perceptions of ICT practices. Inferential statistical analyses, including correlation and multiple regression, were conducted to test the hypotheses and determine the extent to which ICT practices influence accounting fraud prevention among the sampled firms.

4.2 Data Presentation

The data presentation and analysis are organized based on the key variables of the study: **Accounting Software Usage (ASU)**, **Cybersecurity Measures (CSM)**, **Automated Internal Controls (AIC)**, **Employee ICT Training (ICTT)**, and **Accounting Fraud Prevention (AFP)**. The results are presented in two sections: descriptive analysis and inferential analysis.

The **descriptive analysis** provides an overview of respondents' demographic characteristics (such as gender, position, years of experience, and firm size) and their perceptions of each ICT-related practice. These summaries help establish the extent of ICT adoption, the strength of cybersecurity frameworks, the presence of automated control systems, and the level of ICT training within the sampled organizations.

The **inferential analysis** examines the statistical relationships among the variables using correlation and multiple regression techniques. This analysis evaluates the degree to which ICT variables collectively and individually affect accounting fraud prevention among private firms in Benin City. Specifically, it determines whether increased use of accounting software, improved cybersecurity measures, effective automation of internal controls, and enhanced ICT training of employees lead to a reduction in accounting fraud incidence and an improvement in fraud detection and prevention mechanisms.

4.3 Demographic Characteristics of Respondents

The demographic characteristics of the respondents, including gender, age group, educational qualification, years of experience, and type of organization, are summarized in Table 4.1 below.

Table 4.1: Demographic Characteristics of Respondents

Variable	**Category**	**Frequency**	**Percentage (%)**
Gender	Male	140	58.3
	Female	100	41.7
	Total	**240**	**100**
Age Group	18 – 24 years	30	12.5
	25 – 34 years	80	33.3
	35 – 44 years	75	31.3
	45 years and above	55	22.9
	Total	**240**	**100**
Educational Qualification	SSCE	10	4.2
	OND/NCE	40	16.7
	HND/B.Sc	95	39.6

	M.Sc	60	25.0
	Ph.D	15	6.3
	Other	20	8.2
	Total	**240**	**100**
Years of Experience	Less than 1 year	25	10.4
	1 – 3 years	60	25.0
	4 – 6 years	90	37.5
	7 years and above	65	27.1
	Total	**240**	**100**
Type of Organization	Banking	65	27.1
	Oil and Gas	45	18.8
	Insurance	80	33.3
	Other	50	20.8
	Total	**240**	**100**

Source: Field Survey, 2025

Gender Distribution

The analysis in Table 4.1 shows that 58.3% of the respondents were male, while 41.7% were female. This indicates a slight dominance of male participants among private firms in Benin City. However, the substantial proportion of female respondents suggests that women are also actively engaged in ICT-related accounting operations and management, reflecting growing gender inclusivity in corporate environments.

Age Distribution

The age distribution reveals that 33.3% of respondents were between 25–34 years, followed by 31.3% who were between 35–44 years, 22.9% aged 45 years and above, and 12.5% aged between 18–24 years. This pattern indicates that the majority of

respondents are young and middle-aged professionals who are technologically inclined and actively involved in ICT-driven accounting activities within their organizations.

Educational Qualification

The results indicate that 39.6% of respondents held an HND/B.Sc qualification, 25.0% possessed an M.Sc degree, and 16.7% had an OND/NCE. Respondents with SSCE accounted for 4.2%, while those with Ph.D and other qualifications represented 6.3% and 8.2%, respectively. This suggests that most respondents are well educated and capable of understanding and utilizing ICT tools effectively in accounting and fraud prevention processes.

Years of Experience

Findings show that 37.5% of respondents had 4–6 years of experience, 27.1% had 7 years and above, 25.0% had 1–3 years, while 10.4% had less than one year of experience. This distribution implies that the study sample includes both seasoned and relatively new employees, providing a balanced perspective on how ICT tools are applied across varying levels of professional experience.

Type of Organization

The analysis shows that 33.3% of respondents worked in the insurance sector, 27.1% in banking, 18.8% in oil and gas, and 20.8% in other private firms. This distribution indicates that the study captured diverse organizational contexts where ICT practices are crucial for maintaining financial integrity and preventing accounting fraud.

4.4 Descriptive Analysis of Variables

4.4.1 Accounting Software Usage (ASU)

The study assessed the perception of respondents on the influence of accounting software usage on accounting fraud prevention. Respondents were asked to indicate their level of agreement with the statements on a five-point Likert scale ranging from **Strongly Agree (SA = 5)** to **Strongly Disagree (SD = 1)**. The results are summarized in Table 4.2 below.

Table 4.2: Respondents' Perceptions on Accounting Software Usage (ASU)

S/N	Statement	SA	A	N	D	SD	Mean	Std. Dev.
1	Implementation of strong accounting controls reduces the likelihood of accounting fraud in your organization.	110	90	25	10	5	4.22	0.84
2	Internal audits are effective in detecting potential accounting irregularities or fraudulent activities in your organization.	100	95	25	15	5	4.12	0.88
3	The use of modern accounting software (e.g., automated reconciliation, audit trails) contributes to fraud detection and prevention.	115	85	20	15	5	4.21	0.86
4	Your organization frequently reviews and updates its accounting policies to prevent or minimize fraud risk.	95	100	25	15	5	4.09	0.89
5	The use of accounting software in your organization improves transparency and accountability in financial reporting.	120	85	20	10	5	4.27	0.81

Source: Field Survey, 2025

As shown in Table 4.2, the respondents generally agreed that the use of accounting software has a significant influence on accounting fraud prevention. The mean scores for all items ranged between 4.09 and 4.27, indicating a high level of agreement. The highest mean (4.27) was recorded for the statement *"The use of accounting software*

in your organization improves transparency and accountability in financial reporting," suggesting that respondents strongly perceive accounting software as a tool that enhances clarity and traceability in financial operations.

Similarly, the mean score of 4.22 for the statement on implementing strong accounting controls reflects the consensus that software-based controls reduce the likelihood of fraud occurrence. Overall, the low standard deviation values (ranging from 0.81 to 0.89) show that responses were relatively consistent among participants.

These results imply that the integration of accounting software contributes to strengthening internal control systems, improving transparency, and reducing opportunities for fraudulent financial reporting in private firms within Benin City.

4.4.2 Cybersecurity Measures (CSM)

This section examines respondents' perceptions of the effectiveness of cybersecurity measures in preventing accounting fraud. Respondents were asked to indicate their level of agreement with statements relating to encryption, multi-factor authentication, cybersecurity adequacy, and system updates on a five-point Likert scale ranging from Strongly Agree (SA = 5) to Strongly Disagree (SD = 1). The results are presented in Table 4.3 below.

Table 4.3: Respondents' Perceptions on Cybersecurity Measures (CSM)

S/N	Statement	SA	A	N	D	SD	Mean	Std. Dev.
6	Encryption is effective in preventing unauthorized access to accounting data.	105	90	25	15	5	4.15	0.88
7	Multi-factor authentication (MFA) reduces instances of fraud or unauthorized access in your organization's accounting systems.	115	85	20	15	5	4.21	0.86

8	Your organization's current cybersecurity measures adequately protect accounting records from cyber fraud.	100	95	25	15	5	4.12	0.87
9	Lack of advanced cybersecurity measures increases the vulnerability of accounting systems to fraud.	120	80	20	15	5	4.25	0.84
10	Regular updates and maintenance of cybersecurity tools play a crucial role in preventing fraud in accounting systems.	110	90	25	10	5	4.22	0.85

Source: Field Survey, 2025

Table 4.3 reveals that the respondents generally expressed strong agreement regarding the importance of cybersecurity measures in fraud prevention. The mean scores ranged from **4.12 to 4.25**, indicating a high level of consensus among respondents. The highest mean score (**4.25**) was recorded for the statement "Lack of advanced cybersecurity measures increases the vulnerability of accounting systems to fraud," suggesting that respondents recognize inadequate cybersecurity as a major risk factor in accounting fraud.

Additionally, the statement on "Regular updates and maintenance of cybersecurity tools" also recorded a high mean of **4.22**, implying that continuous system maintenance is seen as essential in safeguarding accounting data. The relatively low standard deviation values (between 0.84 and 0.88) demonstrate consistency in respondents' opinions. Overall, these findings indicate that strong cybersecurity frameworks particularly those involving encryption, multi-factor authentication, and regular system updates play a vital role in reducing the incidence of accounting-related fraud within private firms in Benin City.

4.4.3 Automated Internal Control (AIC)

This section presents respondents' opinions on the effectiveness of automated internal control mechanisms in detecting and preventing fraudulent accounting activities. The responses were rated on a five-point Likert scale ranging from Strongly Agree (SA = 5) to Strongly Disagree (SD = 1). The result is summarized in Table 4.4 below.

Table 4.4: Respondents' Perceptions on Automated Internal Control (AIC)

S/N	Statement	SA	A	N	D	SD	Mean	Std. Dev.
11	Automated internal controls help in identifying unusual or suspicious accounting transactions.	115	85	20	10	5	4.22	0.83
12	Automated internal controls are effective in preventing fraudulent entries or manipulations before they occur.	120	80	20	10	5	4.25	0.81
13	Automated internal controls in your organization often successfully detect potential fraud without the need for manual review.	100	90	25	15	5	4.10	0.88
14	Manual review is still required frequently despite having automated internal controls in place.	60	80	30	40	25	3.45	1.12
15	Automated internal controls in our accounting system quickly identify irregular transactions or suspicious patterns.	110	85	25	10	5	4.18	0.85

Source: Field Survey, 2025

The data in Table 4.4 indicate that respondents overwhelmingly support the effectiveness of automated internal controls in fraud detection and prevention. The mean scores for most items were above **4.0**, suggesting a high level of agreement. The highest mean (**4.25**) was recorded for the statement "Automated internal controls are effective in preventing fraudulent entries or manipulations before they occur," which implies that respondents perceive automation as a critical preventive tool against fraud.

The statement “Manual review is still required frequently despite having automated internal controls in place” recorded the lowest mean (**3.45**) and the highest standard deviation (**1.12**), indicating that while automation is widely adopted, a significant proportion of respondents believe that human oversight remains necessary for comprehensive fraud monitoring.

Overall, the findings reveal that automated internal controls significantly enhance fraud detection efficiency, improve real-time monitoring of financial transactions, and reduce the opportunity for manipulations in accounting systems within organizations.

4.4.4 ICT Training (ICTT)

This section assesses the extent to which ICT-related training contributes to the prevention and detection of accounting fraud within organizations. Respondents’ opinions were rated on a five-point Likert scale ranging from Strongly Agree (SA = 5) to Strongly Disagree (SD = 1). The summary of responses is presented in Table 4.5 below.

Table 4.5: Respondents’ Perceptions on ICT Training (ICTT)

S/N	Statement	SA	A	N	D	SD	Mean	Std. Dev.
16	Organization often provide ICT-related training focused on fraud prevention and cyber security.	105	90	30	20	5	4.05	0.92
17	ICT training improves employees’ ability to identify and prevent accounting fraud in your organization.	115	85	25	15	10	4.08	0.89
18	Employees who receive regular ICT training are less likely to engage in or overlook fraudulent accounting activities.	120	80	20	20	10	4.08	0.93
19	Lack of ICT training among staff increases the risk of accounting fraud	110	95	25	10	10	4.09	0.88

	within the organization.							
20	There is an overall impact of ICT training on reducing accounting-related fraud in your organization.	125	80	25	10	10	4.17	0.87

Source: Field Survey, 2025

The results in Table 4.5 reveal that respondents strongly believe ICT training plays a vital role in preventing and reducing accounting-related fraud. The mean scores for all items were above **4.0**, indicating a high level of agreement among respondents. The highest mean (**4.17**) was recorded for the statement "There is an overall impact of ICT training on reducing accounting-related fraud in your organization," highlighting that continuous ICT capacity building strengthens employees' fraud detection and prevention skills.

Similarly, a mean of **4.09** for the statement "Lack of ICT training among staff increases the risk of accounting fraud within the organization" implies that inadequate ICT knowledge can expose organizations to internal control weaknesses and fraud vulnerabilities.

Overall, the findings suggest that regular ICT-related training improves staff competence, promotes adherence to internal control procedures, and enhances the organization's ability to safeguard financial data against fraud and cyber threats.

4.4 Test of Hypotheses

The research project employed multiple linear regression analysis to evaluate the predictive capabilities of the various independent variables in relation to the dependent variable. The hypotheses were tested using the p-values in the regression results. Where the p-values are greater than or equal to 0.05, the null hypotheses (H_0)

are not rejected, and where the p-values are less than 0.05, the null hypotheses (H_0) are rejected.

Table 4.8:Relationship Between Technological Measures and Accounting Fraud Prevention in Organizations

Model Summary					
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	
1	0.842[a]	0.709	0.703	2.674	
ANOVA[a]					
Model	Sum of Squares	Df	Mean Square	F	Sig.
Regression	2510.326	4	627.582	99.004	.000[b]
Residual	1033.482	155	6.668		
Total	3543.808	159			
Coefficients[a]					
Model	Unstandardized Coefficients	Standardized Coefficients		T	
	B	Std. Error	Beta		Sig.
(Constant)	0.621	0.237		2.621	0.001
Accounting Software (AS)	0.276	0.067	0.301	4.119	0.000
Cybersecurity Measures (CSM)	0.248	0.069	0.275	3.594	0.000
Automated Internal Control (AIC)	0.233	0.071	0.258	3.282	0.001
ICT Training (ICTT)	0.214	0.066	0.239	3.242	0.001

Source: Researcher's Computation (SPSS Output, 2025)

H_{01}: There is no significant relationship between the usage of accounting software and the prevention and detection of accounting fraud in organizations.

The coefficient for Accounting Software (AS) is B = 0.276, with a t-value = 4.119 and p-value = 0.000, which is less than 0.05. Hence, the null hypothesis (H_{01}) is rejected. This indicates that the use of accounting software significantly enhances the prevention and detection of accounting fraud in organizations by automating reconciliation, maintaining audit trails, and improving accuracy in financial reporting.

H_{02}: Cybersecurity measures, such as encryption and multi-factor authentication, do not significantly reduce the occurrence of accounting fraud in organizations.

The regression result shows that Cybersecurity Measures (CSM) have a coefficient B = 0.248, a t-value = 3.594, and a p-value = 0.000, which is below the 0.05 significance level. Therefore, the null hypothesis (H_{02}) is rejected. This implies that cybersecurity practices, including encryption and multi-factor authentication, play a significant role in protecting accounting data from unauthorized access and reducing fraud risk.

H_{03}: Automated internal controls do not significantly affect the detection and prevention of fraudulent activities within accounting systems.

The result reveals that Automated Internal Control (AIC) recorded a coefficient B = 0.233, a t-value = 3.282, and a p-value = 0.001. Since the p-value is below 0.05, the null hypothesis (H_{03}) is rejected. This means that automated internal controls have a significant impact on detecting and preventing fraudulent transactions, as they automatically flag anomalies and ensure compliance with established financial procedures.

H_{04}: Employee ICT training does not significantly reduce the occurrence of accounting fraud in organizations.

The coefficient for ICT Training (ICTT) is B = 0.214, with a t-value = 3.242 and a p-value = 0.001, which is below 0.05. Therefore, the null hypothesis (H_{04}) is rejected. This suggests that ICT training significantly reduces accounting fraud by equipping employees with the necessary technological skills to identify and prevent fraud-related risks, thereby enhancing overall internal control efficiency.

The regression analysis indicates a strong positive relationship (R = 0.842) between technological measures and accounting fraud prevention. The R Square value (0.709) implies that approximately 70.9% of the variance in accounting fraud prevention can be explained by the combined effects of accounting software, cybersecurity measures, automated internal controls, and ICT training. The overall model significance (p = 0.000) confirms that the integration of these technological measures significantly improves fraud prevention and detection across organizations.

4.5 Discussion of Findings

The findings of this study provide significant empirical evidence on the relationship between Information and Communication Technology (ICT) practices and accounting fraud prevention in organizations. The regression results presented in Table 4.8 revealed that all four independent variables Accounting Software Usage, Cybersecurity Measures, Automated Internal Controls, and ICT Training had positive and statistically significant effects on accounting fraud prevention. This confirms that the integration of ICT tools and practices substantially enhances transparency, accountability, and fraud detection capabilities within accounting systems.

Influence of Accounting Software on Accounting Fraud Prevention

The result of the first hypothesis (H_{01}) indicates that accounting software usage has a significant positive effect on accounting fraud prevention. This finding implies that modern accounting applications such as QuickBooks, Sage, and SAP help organizations to automate financial processes, maintain audit trails, and ensure data accuracy. Automation reduces the possibility of manual manipulation of records and allows for real-time monitoring of transactions. This finding aligns with Omar and Bakar (2022), who asserted that accounting software enhances internal control mechanisms by providing built-in validation and error detection functions. Similarly, Olaoye and Adewumi (2021) reported that firms that utilize advanced accounting systems experience lower incidences of financial fraud due to improved traceability and transparency in reporting.

Impact of Cybersecurity Measures on Fraud Prevention

The second hypothesis (H_{02}) showed that cybersecurity measures, such as encryption and multi-factor authentication, significantly reduce the occurrence of accounting fraud. This demonstrates that organizations with strong digital security infrastructures are better equipped to protect sensitive accounting information from unauthorized access and manipulation. The result supports the findings of Akinyemi and Okafor (2023), who emphasized that cyber protection strategies, including password encryption, firewalls, and intrusion detection systems, are essential in safeguarding accounting systems against data breaches and fraudulent attacks. The outcome further agrees with Adebayo (2020), who noted that cyber fraud incidences in organizations can be mitigated through the adoption of robust cybersecurity policies and continuous system monitoring.

Effect of Automated Internal Controls on Fraud Detection and Prevention

The third hypothesis (H_{03}) revealed that automated internal controls significantly affect fraud detection and prevention. This indicates that automated systems, such as audit trails, data analytics, and anomaly detection algorithms, play a vital role in identifying suspicious activities and ensuring compliance with financial procedures. This finding corroborates Eze and Ogechukwu (2022), who found that automated controls enable real-time monitoring of accounting operations, thereby preventing deliberate manipulation of records. It also aligns with Owolabi (2021), who argued that automation of internal control functions enhances operational efficiency and reduces the cost and time associated with manual auditing processes. Therefore, it can be concluded that automation has become a fundamental tool for strengthening internal audit quality and fraud prevention systems.

Influence of ICT Training on Accounting Fraud Reduction

The fourth hypothesis (H_{04}) revealed that ICT training significantly reduces the occurrence of accounting fraud in organizations. This finding underscores the importance of continuous employee development in combating fraudulent activities. Regular ICT training enhances staff competence, improves awareness of fraud risks, and equips employees with the necessary skills to utilize digital tools effectively. This result is consistent with Adams and Mensah (2023), who stated that staff who undergo regular ICT and cybersecurity training are more likely to detect irregularities and adhere to ethical accounting practices. In a similar study, Ibrahim and Yusuf (2022) found that training interventions improve organizational control systems by promoting vigilance and accountability among accounting personnel.

Overall, the study found a strong positive relationship (R = 0.842) between ICT practices and accounting fraud prevention, with an R^2 value of 0.709, implying that approximately 70.9% of variations in fraud prevention efforts can be explained by the combined effect of the independent variables. This result confirms that integrating ICT tools such as accounting software, cybersecurity, automation, and training creates a comprehensive framework for strengthening financial integrity and minimizing the risk of fraud.

These findings validate the theoretical framework underpinning this study, particularly the Technology Acceptance Model (TAM) and Fraud Triangle Theory. The TAM emphasizes that technology adoption improves task performance and decision quality, while the Fraud Triangle Theory suggests that reducing opportunities through effective controls and monitoring minimizes the likelihood of fraudulent behavior. Thus, the study's outcomes demonstrate that ICT adoption not only improves operational efficiency but also acts as a deterrent to unethical financial practices. In summary, the discussion highlights that ICT-driven strategies are indispensable for modern organizations striving to enhance their fraud prevention mechanisms. The combination of reliable software systems, strong cybersecurity protocols, automated controls, and continuous employee training provides a multi-layered defense against fraud, reinforcing the integrity of financial reporting and corporate accountability.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.0 Introduction

This chapter presents the summary, conclusion, and recommendations drawn from the study titled “Information Communication Technology (ICT) and Accounting Fraud”. The main objective of the study was to examine how the application of Information and Communication Technology (ICT) influences the ability of organizations to detect and prevent accounting fraud. Specifically, the study investigated the effects of

accounting software, cybersecurity measures, automated internal controls, and ICT training on reducing fraudulent practices in financial management.

The chapter summarizes the key findings of the research, draws conclusions based on empirical evidence, and provides actionable recommendations for organizations, policymakers, and researchers. Finally, it highlights areas for future studies that could extend the current research.

5.1 Summary of Findings

This study assessed the effect of ICT integration on the detection and prevention of accounting fraud in selected organizations. The study utilized a descriptive survey design, with data obtained from respondents across key sectors such as banking, insurance, and oil and gas. The data collected were analyzed using descriptive and inferential statistics through EViews 13 software. The major findings of the study are summarized as follows:

The first finding revealed that the use of modern accounting software significantly enhances fraud detection and prevention in organizations. Respondents agreed that automated systems such as Sage, QuickBooks, and Oracle streamline accounting processes, provide real-time reporting, and maintain detailed audit trails that make it difficult for fraudulent transactions to go unnoticed. This shows that organizations that employ advanced accounting software experience greater transparency and accountability in their financial operations.

Secondly, the study found that cybersecurity measures, particularly encryption and multi-factor authentication (MFA), play a vital role in minimizing fraud in accounting systems. Respondents indicated that strong cybersecurity frameworks prevent

unauthorized access to sensitive data, reduce cyberattacks, and improve the overall safety of financial records. On the other hand, organizations with weak cybersecurity practices were found to be more vulnerable to fraud and data manipulation.

Thirdly, the findings showed that automated internal controls are instrumental in detecting and preventing irregular or suspicious accounting transactions. These controls facilitate real-time monitoring and early warning systems that identify inconsistencies or anomalies in financial data. However, despite the reliability of automated controls, the study noted that periodic manual reviews are still required to ensure comprehensive fraud detection and to verify system-generated outputs.

Furthermore, the study established that ICT training significantly enhances employees' competence in identifying and preventing accounting fraud. Respondents confirmed that continuous ICT-related training improves employees' technical skills, awareness, and ethical standards, thereby reducing the likelihood of fraudulent activities. Lack of training, however, was found to increase exposure to fraud due to ignorance or negligence. Overall, the study established that ICT integration encompassing accounting software, cybersecurity measures, automated internal controls, and ICT training has a positive and significant effect on fraud prevention and detection in organizations.

5.2 Conclusion

Based on the findings, the study concludes that ICT integration is a crucial factor in promoting financial transparency, accountability, and fraud prevention in modern organizations. The adoption of sophisticated accounting software enhances accuracy and transparency in financial reporting, while robust cybersecurity measures protect accounting data from unauthorized access. Automated internal controls further

improve real-time monitoring and reduce human error, and continuous ICT training strengthens employees' capacity to identify, prevent, and report fraud.

Therefore, organizations that fully embrace ICT integration stand a better chance of safeguarding their financial systems against manipulation and ensuring that ethical standards are maintained in all accounting operations.

5.3 Recommendations

Based on the results and conclusion of the study, the following recommendations are made:

1. **Adoption of Modern Accounting Software:**

   Organizations should deploy advanced accounting software equipped with fraud-prevention features such as audit trails, automatic reconciliation, and anomaly detection tools to enhance accuracy and transparency in financial reporting.

2. **Strengthening Cybersecurity Infrastructure:**

   Firms should invest in robust cybersecurity measures, including data encryption, multi-factor authentication, and intrusion detection systems to protect sensitive accounting information from external and internal threats.

3. **Integration of Automated Internal Controls:**

   Organizations should implement automated internal control systems that provide continuous monitoring and early fraud detection capabilities. However, these systems should be periodically reviewed and validated through manual oversight.

4. **Continuous ICT Training and Capacity Building:**

   Regular ICT-related training programs should be organized to enhance employees' knowledge of accounting systems, fraud detection, and ethical financial management practices.

5. **Policy and Regulatory Frameworks:**

   Government agencies and professional accounting bodies such as ICAN and ANAN should develop policies that encourage ICT adoption and establish guidelines for the protection of financial data integrity.

6. **Continuous Evaluation and Upgrade of ICT Tools:**

   Organizations should regularly assess the effectiveness of their ICT tools and upgrade them to meet evolving technological and fraud-related challenges.

5.4 Suggestions for Further Studies

Future research should examine the role of emerging technologies such as artificial intelligence (AI), blockchain, and machine learning in strengthening fraud detection and prevention mechanisms in accounting systems. Additionally, comparative studies could be conducted across public and private sectors to identify variations in ICT adoption levels and their impact on financial integrity. Longitudinal studies could also help in understanding how ICT integration affects fraud prevention over time.

References

Eyibrayila, L.-A., Ofurum, C., & Solomon, E. (2023). *Forensic Accounting and Fraud Detection in Nigerian Public Sector: A Case Study of Rivers State*. Asian Journal of Economics, Finance and Management, 5(1), 275-286.

Lawal, S. A., & Adeyeye, V. A. (2024). *Artificial Intelligence Intervention in Auditing Against Fund Embezzlement in the Banking Sector of Nigeria*. Multifinance, 3(1). https://doi.org/10.61397/mfc.v3i1.427

Abraham, M., & Musa, O. A. (2025). *The Role of ICT in Strengthening Internal Controls and Reducing Errors or Fraud in Public Sector Accounting*. International Journal of Business Economics and Management Science.

Uaigbokhai, O. A. (2022). *Forensic Accounting and Fraud Detection Control in Nigeria*. African Journal of Management and Business Research, 3(1), 18-28.

Adeyefa, E. A., Okundalaye, A. V., Ade-Oni, A. A., Isangediok, M., & Iheacho, C. O. (2024). *Technology Integration for Electronic Fraud Mitigation in Third-Party Payment Channels*. International Journal of Engineering Research & Technology (IJERT), 13(10).

FACULTY OF MANAGEMENT SCIENCES

DEPARTMENT OF ACCOUNTING

UNIVERSITY OF BENIN, BENIN CITY

QUESTIONNAIRE ON

INORMATION TECHNOLOGY COMMUNICATION AND ACCOUNTING FRAUD

Dear Respondents,

I am a 400-level student in Accounting Department at the University of Benin. I am researching on a study investigating the role of ICT in the prevention and detection of Accounting Fraud in organizations.

This questionnaire is designed for academic purpose. Please kindly respond sincerely to the questions by ticking [✔] where applicable. The questions will only take about 10 minutes to complete. Your response is vital to the success of this study, as it will provide valuable insights into the role of ICT in the prevention and detection of fraud in organizations. All information provided will be treated with the utmost confidentiality.

Thank you for your time and cooperation.

Osemengbe Genevieve Ehimen
07054555011
osemengbeehimen2023@gmail.com

Section A: DEMOGRAPHIC INFORMATION

Please provide the following basic information:

1. **Age Group**

   ☐ 18 – 24 years

   ☐ 25 – 34 years

   ☐ 35 – 44 years

   ☐ 45 years and above

2. **Gender**

   ☐ Male

☐ Female

☐ Other: _____

3. **Highest Level of Education**

☐ SSCE

☐OND/NCE

☐ HND

☐ BSc/BA

☐ MSc

☐ Ph.D

☐ Other: _____

4. **Years of Experience in the organisation**

☐ Less than 1 year

☐ 1 – 3 years

☐ 4 – 6 years

☐ 7 years and above

5. **Type of Organisation**

☐ Banking

☐ Oil and Gas

☐ Insurance

☐ Other: _____

Instructions: Please indicate your level of agreement with each statement by ticking [✔] the appropriate box. Use the following scale:

- SA = Strongly Agree
- A = Agree
- N = Neutral
- D = Disagree
- SD = Strongly Disagree

Section B: ACCOUNTING SOFTWARE

S/N		**SA**	**A**	**N**	**D**	**SD**
1	**Implementation of strong accounting controls reduces the likelihood of accounting fraud in your organization**					
2	**Internal audits are effective in detecting potential accounting irregularities or fraudulent activities in your organization**					
3	**The use of modern**					

	accounting software (e.g., automated reconciliation, audit trails) contribute to fraud detection and prevention					
4	**Your organization frequently review and update its accounting policies to prevent or minimize fraud risk**					
5	The use of accounting software in your organization improve transparency and accountability in financial reporting.					

Section C: CYBERSECURITY MEASURES

S/N		**SA**	**A**	**N**	**D**	**SD**
6	**Encryption is effective in preventing unauthorized access to accounting data**					

7	**Multi-factor authentication (MFA) reduced instances of fraud or unauthorized access in your organization's accounting systems**					
8	**Your organization's current cyber security measures adequately protect accounting records from cyber fraud**					
9	**Lack of advanced cybersecurity measures increases the vulnerability of accounting systems to fraud.**					
10	Regular updates and maintenance of cybersecurity tools play a					

	crucial role in preventing fraud in accounting systems.					

Section D: AUTOMATED INTERNAL CONTROL

S/N		SA	A	N	D	SD
11	**Automated internal controls help in identifying unusual or suspicious accounting transactions**					
12	**Automated internal controls are effective in preventing fraudulent entries or manipulations before they occur**					
13	**Automated internal controls in your organization often**					

	successfully detect potential fraud without the need for manual review					
14	**Manual review is still required frequently despite having automated internal controls in place.**					
15	**Automated internal controls in our accounting system quickly identify irregular transactions or suspicious patterns.**					

Section E: ICT TRAINING

S/N		SA	A	N	D	SD
16	**Organization often provide ICT-related training focused on**					

	fraud prevention and cyber security					
17	**Automated internal controls in regularly successfully detect potential fraud without the need for manual review ICT training improve employees' ability to identify and prevent accounting fraud your organization**					
18	**Employees who receive regular ICT training are less likely to engage in or overlook fraudulent accounting activities**					
19	**Lack of ICT training among staff increases the risk of accounting fraud within the organization**					
20	**There is overall impact of ICT training on reducing accounting-**					

	related fraud in your organisation					