PAPER NAME

SOPHIA OKORO CORRECTED.docx

WORD COUNT

21733 Words

CHARACTER COUNT

133601 Characters

PAGE COUNT

134 Pages

FILE SIZE

350.7KB

SUBMISSION DATE

Oct 23, 2025 3:52 PM GMT+1

REPORT DATE

Oct 23, 2025 3:54 PM GMT+1

20% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 15% Internet database
- 7% Publications database
- Crossref database
- 16% Submitted Works database

Excluded from Similarity Report

- Crossref Posted Content database
- Bibliographic material
- Quoted material
- Cited material
- Small Matches (Less then 8 words)

INFORMATION AND COMMUNICATION TECHNOLOGY(ICT) AND ACCOUNTING FRAUD

BY

Sophia Osasere OKORO
MGS2104627

DEPARTMENT OF ACCOUNTING
FACULTY OF MANAGEMENT SCIENCES
UNIVERSITY OF BENIN

OCTOBER, 2025

INFORMATION AND COMMUNICATION TECHNOLOGY(ICT) AND ACCOUNTING FRAUD

BY

Sophia Osasere OKORO
MGS2104627

A RESEARCH PROJECT SUBMITTED TO THE DEPARTMENT OF ACCOUNTING, FACULTY OF MANAGEMENT SCIENCES, UNIVERSITY OF BENIN IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF BACHELOR OF SCIENCE DEGREE IN ACCOUNTING OF THE UNIVERSITY OF BENIN, BENIN CITY.

OCTOBER, 2025.

DECLARATION

I, **Sophia Osasere OKORO**, do hereby declare that this project work is entirely my work and composition under the supervision of Dr. Samuel Umanah. This work has not been previously submitted for award of a degree elsewhere. All references made to the work of others have been duly acknowledged.

_____ _____

Sophia Osasere OKORO **Date:**
MGS2104627
Project Student

CERTIFICATION

This is to certify that this research work submitted by **Sophia Osasere OKORO** with matriculation number **MGS2104627** to the Department of Accounting, Faculty of Management Sciences, University of Benin, Benin city under the full supervision of Dr. Samuel Umanah and in accordance with the requirements of the Department of Accounting of the University of Benin, Benin City is adequate in scope and quality for the Award of Bachelor of Sciences Degree in Accounting.

Dr. Samuel Umanah **Date:**
Project Supervisor.

Dr.Godstime O. Ikhu. Omoregbe **Date:**
Project Coordinator

Prof.Osasu Obaretin **Date:**
Head of Department

DEDICATION

This project is dedicated to Almighty God for His grace, for seeing me throughout the course of this programme and the ease He gave me for the completion of this programme. I also dedicated this project to my wonderful Parents, Mr Roger Okoro Erharuyi and Mrs Stella Okoro Amenaghawon, for their love, advice and relentless effort towards my education.

ACKNOWLEDGEMENTS

My unending gratitude is to God Almighty for his grace and mercies upon my life, his unending love and strength to carryout this research till completion

My sincere appreciation goes to my project Supervisor, Dr. Samuel Umanah, for the guidance, advice and the corrections, and also for making the course of completing this programme a success.

I also express profound gratitude to my Head of Department Prof. Osasu Obaretin, my project coordinator Dr.Godstime O. Ikhu. Omoregbe and all lecturers in accounting department who contributed one way or the other to make this programme a success.

My heartfelt gratitude goes to my parents, Mr Roger Okoro Erharuyi and Mrs Stella Okoro Amenaghawon, for their love, advice, prayers and support morally and financially. I also want to appreciate my siblings Okoro Iyore Jennifer and Okoro Adesuwa precious for their support in this programme.

To my wonderful friends Augustine Blessing Oshuware and Ivharue O. Paul, thank you very much and I love you all. May God bless every area of your lives. Thanks to my course mates and every other person who in one way or the other contributed to the success of this programme, I am sincerely grateful and may God bless you all.

TABLE OF CONTENTS

ABSTRACT

The study examines the impact of Information and Communication Technology (ICT) on accounting fraud prevention in private firms. The research investigates the use of various ICT tools, including accounting software, cybersecurity measures, automated internal controls, and employee ICT training, and their roles in detecting and preventing fraudulent activities. The research instrument used in this study includes surveys and questionnaires administered to accounting professionals across selected private firms in Benin City, Edo State, Nigeria. The findings indicate that accounting software, when effectively implemented, enhances data accuracy and reduces fraud. Cybersecurity measures, such as encryption and multi-factor authentication, also play a critical role in protecting financial data. Additionally, automated internal controls significantly limit opportunities for fraud, while employee ICT training helps in recognizing fraud risks and adhering to ethical standards. Based on these findings, the study recommends that private firms invest in comprehensive ICT systems, continuous employee training, and strong cybersecurity measures to strengthen their fraud prevention frameworks and enhance organizational integrity.

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

In the modern company environment, Information communication Technology (ICT) underpins organisational accounting systems, facilitating the efficient processing, storage, and transfer of financial data. The extensive implementation of ICT has fundamentally altered conventional accounting procedures by automating repetitive tasks, improving data precision, and facilitating real-time decision-making. Empirical research indicates that technologies like accounting software, Enterprise Resource Planning (ERP) systems, and cloud-based platforms enable the seamless integration of financial data across organisational units, thereby enhancing financial management and operational efficiency (Rekhi & Johri, 2024); (Mobilingo & Hailah, 2024); (Ali et al., 2024).

The digitisation of accounting records and the implementation of ICT have facilitated the automation of procedures such as bookkeeping, payroll, and financial reporting, which formerly depended on labour-intensive manual entry. This transition has significantly diminished human error and enhanced the dependability of financial data, facilitating compliance with regulatory mandates (Ahmad et al., 2023); (Werastuti et al., 2023). Moreover, real-time access to centralised financial data via ERP and cloud-based solutions enables managers to make quicker and more informed business choices (Ali et al., 2024); (Rathakrishnan & Baskar, 2024).

Notwithstanding these gains, the digital revolution of accounting processes presents new concerns, particularly with accounting fraud. The shift to ICT-based systems has resulted in advanced techniques for altering financial records, as digital platforms introduce new weaknesses that fraudsters can exploit (Efuntade & Efuntade, 2023; Tuharea et al., 2024). Prevalent fraudulent behaviours encompass asset misappropriation, statement fabrication, and corruption, which can be exacerbated by deficiencies in digital controls and inadequate oversight (Adekola et al., 2024). As organisations transition to increasingly intricate ICT environments, the threat of unauthorised access, cyberattacks, and the manipulation of digital information has emerged as a significant worry (Rathakrishnan & Baskar, 2024); (Judijanto & Defitri, 2024). Research indicates that the escalating complexity and automation of accounting processes necessitate stringent internal controls, ongoing monitoring, and regular system audits to maintain financial data integrity and avert fraudulent actions (Subedi & Neupane, 2024); (Vutumu, 2024). Inadequate security measures in digital accounting systems may unintentionally enable the hiding and manipulation of transactions (Efuntade & Efuntade, 2023).

Positively, ICT offers robust resources for the detection and prevention of fraud. The application of advanced data analytics, forensic accounting methods, machine learning, and artificial intelligence (AI) markedly enhances an organization's capacity to detect, oversee, and address fraudulent activities (Adelakun et al., 2024; Ahmad et al., 2023; Prihanto et al., 2024). Forensic accounting currently utilises digital techniques such anomaly detection algorithms, data mining, and continuous auditing systems, which are

crucial for real-time fraud detection and minimising false positives (Ali et al., 2024); (Dewayanto, 2023). Blockchain technology is emerging as a disruptive instrument in accounting, providing immutable records and transparent transaction histories that enhance audit trails and prevent fraudulent modifications (Rekhi & Johri, 2024). Automated warnings and AI-driven monitoring enable organisations to swiftly identify suspicious activities, while cloud-based systems provide safe, centralised access to financial data, enhancing oversight and response time (Mobilingo & Hailah, 2024); (Werastuti et al., 2023).

Cybersecurity protocols like as firewalls, encryption, and multi-factor authentication are essential for safeguarding digital accounting systems against unauthorised access and external threats (Rathakrishnan & Baskar, 2024). Research constantly emphasises the necessity of ongoing employee ICT training, which mitigates the risk of inadvertent breaches and equips staff to recognise phishing efforts and social engineering strategies (Rekhi & Johri, 2024); (Eghe-Ikhurhe et al., 2024). Empirical research in various nations and organisational settings validates the efficacy of ICT and forensic accounting instruments in the prevention and detection of fraud. A cross-national analysis revealed that the implementation of rigorous forensic accounting methods alongside sophisticated ICT is associated with reduced occurrences of financial fraud, particularly in contexts with robust regulatory frameworks and anti-corruption legislation (Idrus et al., 2024). Studies in both public and commercial sectors substantiate the importance of internal controls, ongoing monitoring, and whistleblower mechanisms, all of which are significantly

augmented by digital technology (Tuharea et al., 2024); (Subedi & Neupane, 2024). Moreover, literature reviews and bibliometric analyses indicate a shift towards more advanced, interdisciplinary strategies for fraud prevention, emphasising the necessity for continuous education, regulatory adjustments, and international collaboration in the application of forensic accounting and ICT tools (Judijanto & Defitri, 2024); (Dewayanto, 2023). These studies promote ongoing innovation in technology and governance to guarantee that accounting systems stay robust against advancing fraud methods. The incorporation of ICT into accounting procedures has markedly enhanced the management, transparency, and accuracy of financial data, while concurrently creating new hazards that necessitate diligent scrutiny and innovation. The literature unequivocally indicates that the most efficacious fraud prevention and detection systems integrate advanced digital technologies, including AI, blockchain, and cloud platforms, with robust internal controls, consistent employee training, and proactive organisational cultures (Rekhi & Johri, 2024); (Adelakun et al., 2024); (Mobilingo & Hailah, 2024); (Rathakrishnan & Baskar, 2024). Organisations aiming to reduce accounting fraud risks and promote financial integrity must prioritise the strategic implementation of ICT, complemented by continuous research and training.

1.2 Statement of the Research Problem

The use of Information and Communication Technology (ICT) tools into accounting systems has significantly enhanced efficiency, transparency, and accuracy in financial reporting across global organisations (Rekhi & Johri, 2024); (Ali et al., 2024). This

increasing reliance on digital solutions in accounting has concurrently created new vulnerabilities, especially regarding accounting fraud and cybercrime (Efuntade & Efuntade, 2023; Rathakrishnan & Baskar, 2024). As fraudsters persistently innovate methods to exploit vulnerabilities in ICT infrastructure, organisations must rigorously evaluate and modify their technological defences to guarantee efficient fraud prevention and detection (Adelakun et al., 2024); (Ahmad et al., 2023).

Notwithstanding significant progress such as the extensive implementation of accounting software, Enterprise Resource Planning (ERP) systems, comprehensive cybersecurity measures, and employee ICT training apprehensions remain regarding the true efficacy of these instruments in reducing accounting fraud (Mobilingo & Hailah, 2024). Research indicates that although ERP systems centralise data and automate processes to enhance financial transparency, they remain vulnerable to unauthorised access and advanced cyber threats if security protocols are inadequate (Efuntade & Efuntade, 2023; Rathakrishnan & Baskar, 2024). Likewise, whereas fraud detection tools and advanced analytics improve reporting and monitoring functions, they do not consistently resolve enduring issues such as human mistake, deliberate manipulation, or staff cooperation (Ali et al., 2024); (Dewayanto, 2023).

The sophistication of contemporary cyberattacks is increasing, focussing on the technological framework supporting financial systems and making even the most advanced security protocols vulnerable to breaches (Adelakun et al., 2024); (Werastuti et al., 2023). Empirical reviews indicate that technologies like blockchain and AI are increasingly

utilised for their potential to enhance detection and fortify audit trails; however, their effectiveness is significantly contingent upon the quality of implementation and ongoing updates to combat emerging fraud techniques (Rekhi & Johri, 2024); (Prihanto et al., 2024). A significant shortcoming of much existing research is that ICT is frequently regarded as a homogeneous category, thereby concealing the distinct advantages and disadvantages of particular technologies. The unique role of staff ICT training in fraud prevention is significantly underexamined, despite increasing evidence that user awareness and digital literacy are essential for ensuring system security (Eghe-Ikhurhe et al., 2024; Rathakrishnan & Baskar, 2024).

This research aims to empirically examine the distinct effects of several ICT tools specifically, accounting software, ERP systems, cybersecurity measures, and employee ICT training on the prevention and detection of accounting fraud. The study seeks to elucidate the impact of each component, aiming to optimise these tools to mitigate fraudulent behaviour and bolster organisational integrity (Subedi & Neupane, 2024); (Mobilingo & Hailah, 2024).

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. Does employee ICT training significantly reduce the occurrence of accounting fraud in organizations?

1.4 Research Objectives

The Main Objective of the Study is to examine the impact of information communication technology ICT and accounting fraud, 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:

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

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

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

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

1.6 Scope of the Study

This study will focus specifically on private firms operating within Benin City, Edo State, Nigeria. 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. The study will concentrate on four key ICT variables: accounting software usage, cybersecurity measures, automated internal controls, and employee ICT training. Each variable will be analyzed independently to determine its specific impact on the frequency and nature of accounting fraud incidents within private firms.

To achieve this, the study will employ a quantitative research approach, with data collected primarily through structured questionnaires. These questionnaires will be distributed to key personnel involved in accounting and financial management within the selected firms, including financial officers, internal auditors, and accounting staff. By focusing on private enterprises in Benin City, the study aims to provide localized and practical insights that can guide firms in the region in strengthening 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

While this study aims to provide a comprehensive understanding of how Information and Communication Technology (ICT) contributes to the detection and prevention of accounting fraud in Nigeria, it is important to acknowledge certain limitations that may affect the scope, accuracy, and generalizability of the findings. These limitations do not undermine the validity of the research but rather offer context for interpreting its results.

1. **Limited Access to Sensitive Data:**Due to the confidential nature of financial records and fraud-related information, some organizations may be reluctant to disclose accurate or complete data.

2. **Respondent Bias:**Participants may withhold information or provide socially desirable responses, particularly when discussing fraud or weaknesses in their ICT systems.

3. **Technological Diversity:**The disparity in ICT adoption and sophistication among different organizations may limit the ability to generalize findings across the broader Nigerian accounting sector.

4. **Geographical Scope:**The study may be restricted to a specific region or a limited number of organizations, which may not fully represent the national context.

5. **Time Constraints:**The duration allocated for this research might restrict the depth of data collection and analysis, especially where more extensive fieldwork is required.

6. **Rapid Technological Changes:**As ICT tools evolve quickly, some findings may become obsolete shortly after the study, especially in a dynamic field like technology and fraud detection.

7. **Lack of Standardization:**Inconsistencies in how fraud is defined or how ICT effectiveness is measured across different organizations can make it difficult to compare results uniformly.

1.9 Definition of Terms

1. **Information Communication Technology (ICT):** ICT refers to a broad range of technological tools and resources used to transmit, store, create, share, or manage information. In the context of accounting, ICT includes systems like accounting software, ERP platforms, cybersecurity tools, and digital communication channels that enhance financial data management (Molla, 2020).

2. **Accounting Fraud:** Accounting fraud is the intentional manipulation, misstatement, or omission of financial data to deceive stakeholders. It includes activities such as falsification of records, asset misappropriation, and fraudulent financial reporting (Bhasin, 2020).

3. **Accounting Software:** This refers to computer programs used to manage financial transactions and records. Such software automates bookkeeping, payroll, invoicing, and financial reporting processes, improving accuracy and reducing manual errors (Adebisi & Alao, 2021).

4. **Enterprise Resource Planning (ERP) Systems:** ERP systems are integrated management platforms that combine various business processes, including

accounting, into a single database and user interface. They enable real-time monitoring and control of financial and operational data across departments (Al-Faki, 2021).

5. **Cybersecurity Measures:** These are protective strategies and tools used to secure systems, networks, and data from cyber threats or unauthorized access. Examples include firewalls, encryption, antivirus software, and multi-factor authentication (Nguyen & Huynh, 2021).

6. **Automated Internal Controls:** These are pre-programmed procedures embedded within ICT systems that automatically monitor and enforce compliance with accounting policies and practices. They detect irregularities, limit user access, and ensure real-time validation of transactions (Li & Li, 2020).

7. **Employee ICT Training:**This involves structured learning programs aimed at improving employees' knowledge and skills in using ICT tools safely and effectively. It includes training on system usage, data security protocols, and fraud awareness (Teixeira & Souza, 2020).

CHAPTER TWO

2.1 Introduction

This chapter reviewed the related literature of the study, it starts by reviewing conceptually the variables of the study, it further reviewed relevant theories and finally reviewed related empirical studies.

2.2 Conceptual Review

2.2.1 Accounting Fraud

Accounting fraud is a pervasive and evolving threat that undermines the integrity, reliability, and credibility of financial reporting across both public and private organizations. It encompasses a spectrum of intentional acts committed by individuals or groups to misrepresent financial information, conceal losses, inflate profits, or manipulate accounting records for personal or organizational gain. The consequences of accounting fraud are far-reaching, often resulting in severe financial losses, damaged reputations, regulatory sanctions, and diminished stakeholder trust (Adekola et al., 2024); (Tuharea et al., 2024). In today's complex business environment, the detection, prevention, and management of accounting fraud have become top priorities for organizations, regulators, and auditors alike. Accounting fraud typically manifests through several primary methods: manipulation of financial statements, misappropriation of assets, corruption, and fraudulent disclosures. Manipulation of financial statements such as overstating revenues,

understating expenses, or omitting liabilities is often executed to present a falsely positive financial position to investors, lenders, or regulatory authorities. Asset misappropriation involves the theft or unauthorized use of organizational resources, which may include embezzlement of cash, misuse of company credit cards, or unauthorized transfer of assets. Corruption, on the other hand, encompasses bribery, kickbacks, and conflicts of interest, where individuals leverage their positions for illicit gain at the expense of the organization (Ali et al., 2024); (Werastuti et al., 2023).

The proliferation of digital technologies and sophisticated accounting systems has, paradoxically, both improved the capacity for detecting fraudulent activities and introduced new avenues for perpetrating fraud. Automated accounting systems and digital platforms, while enhancing efficiency and data integrity, may also contain exploitable weaknesses if not properly configured and monitored (Adelakun et al., 2024); (Rekhi & Johri, 2024). Cybercriminals increasingly exploit vulnerabilities in accounting software, ERP systems, and cloud-based solutions to manipulate data, alter digital records, or gain unauthorized access to sensitive financial information (Rathakrishnan & Baskar, 2024). Fraudulent schemes often involve a combination of deliberate circumvention of internal controls, collusion among employees, and sophisticated techniques such as falsified documentation or fictitious transactions. The increasing complexity and speed of digital transactions can make fraud more difficult to detect, especially when organizational

controls are inadequate or when staff lack the requisite training to recognize warning signs (Eghe-Ikhurhe et al., 2024).

The consequences of accounting fraud extend well beyond financial loss. High-profile cases of fraud have led to bankruptcies, legal proceedings, industry reforms, and significant erosion of public trust in financial reporting. Regulators and standard-setting bodies have responded by tightening reporting requirements, enhancing oversight mechanisms, and demanding more transparency in financial disclosures. As a result, the responsibility for fraud prevention and detection now rests not only with auditors and regulators but also with organizational leadership, internal auditors, and every employee involved in financial processes (Tuharea et al., 2024). One of the most powerful tools in combating accounting fraud is forensic accounting, which involves the use of specialized investigative techniques, advanced data analytics, and digital forensics to uncover, analyze, and document fraudulent activities (Ali et al., 2024). Forensic accountants leverage machine learning and artificial intelligence to analyze large datasets, detect anomalies, and identify patterns consistent with fraud. These technological advances allow for proactive fraud detection, enabling organizations to respond to suspicious activities in real time and to strengthen internal controls accordingly (Adelakun et al., 2024).

Internal controls also serve as a primary line of defense, encompassing policies and procedures designed to prevent unauthorized transactions, segregate duties, and ensure accurate record-keeping. The automation of internal controls within accounting systems

such as approval workflows, transaction monitoring, and audit trails significantly reduces the opportunities for fraud by limiting manual intervention and ensuring accountability (Werastuti et al., 2023); (Mobilingo & Hailah, 2024). Another critical dimension of accounting fraud prevention is organizational culture and employee training. Employees who understand the importance of ethical conduct, confidentiality, and vigilance are less likely to participate in or inadvertently enable fraudulent activities. Comprehensive ICT training and regular awareness campaigns help staff recognize red flags, adhere to best practices, and contribute to an environment where fraud is less likely to occur (Eghe-Ikhurhe et al., 2024).

Globally, organizations are increasingly collaborating with regulatory bodies, adopting international accounting standards, and leveraging global best practices to strengthen their defenses against accounting fraud. Industry research highlights the importance of continuous adaptation, as fraudsters constantly devise new methods to exploit emerging technologies and circumvent controls (Judijanto & Defitri, 2024). Accounting fraud remains a complex, multifaceted risk that requires coordinated action from technology, people, and governance structures. Through a combination of advanced forensic techniques, robust internal controls, proactive employee training, and a strong ethical culture, organizations can better detect, prevent, and respond to fraudulent activities, thereby safeguarding their financial integrity and stakeholder confidence (Adekola et al., 2024); (Tuharea et al., 2024); (Ali et al., 2024); (Adelakun et al., 2024).

2.2.2 Information Communication Technology

Information Communication Technology (ICT) encompasses a broad range of technologies that facilitate the collection, processing, storage, and dissemination of information within and across organizations. In recent years, the evolution of ICT has revolutionized business operations, particularly in the accounting field, by integrating digital systems that streamline processes, enhance data accuracy, and foster greater connectivity. ICT is not limited to computers and basic office software; it includes advanced digital tools such as cloud computing, mobile applications, blockchain technology, artificial intelligence (AI), data analytics platforms, and secure communication networks. These technologies collectively support the efficient management of organizational resources, promote information sharing, and improve the overall decision-making process (Rekhi & Johri, 2024). The impact of ICT on accounting functions is particularly profound. The adoption of cloud-based solutions enables real-time access to financial data from any location, facilitating remote work and collaborative financial management. Furthermore, the integration of ERP systems brings together disparate business processes into a unified platform, allowing seamless sharing of data across departments and ensuring consistency in financial reporting (Mobilingo & Hailah, 2024). Artificial intelligence and machine learning algorithms are now being used to automate routine accounting tasks, such as invoice processing and payroll management, which not only reduces manual errors but also frees up professionals to focus on more complex,

value-adding activities (Adelakun et al., 2024). Data analytics tools provide accountants with powerful capabilities to extract actionable insights from large datasets, helping organizations identify financial trends, predict future outcomes, and detect anomalies that could indicate fraudulent activities (Ahmad et al., 2023).

Security and integrity of data are central concerns in ICT, especially as the volume of sensitive information managed by organizations grows. Robust cybersecurity frameworks, including encryption, firewalls, and multi-factor authentication, have become essential to safeguard data from unauthorized access and cyber threats. As digital attacks become increasingly sophisticated, organizations are investing in continuous monitoring systems and employee ICT training programs to reduce vulnerabilities and enhance the resilience of their digital infrastructure (Rathakrishnan & Baskar, 2024). The emergence of blockchain technology in accounting represents another significant advancement, providing immutable records and enhancing transparency in transactions, which helps to reinforce trust and accountability in financial reporting (Rekhi & Johri, 2024). ICT's influence extends to organizational culture, enabling new ways of working and fostering a collaborative environment. The use of instant messaging platforms, videoconferencing, and document-sharing tools has made communication more efficient and supported the development of virtual teams. Additionally, the digitalization of training and development through e-learning platforms ensures that employees can continuously update their ICT

competencies, keeping pace with technological advancements and compliance requirements (Eghe-Ikhurhe et al., 2024).

Research also points to the growing necessity for a strategic approach to ICT integration, emphasizing not only technology adoption but also governance, policy frameworks, and ongoing evaluation of system effectiveness. Organizations are increasingly aware that the benefits of ICT such as improved productivity, enhanced financial integrity, and robust fraud detection are maximized when technological solutions are supported by a skilled workforce and strong internal controls (Subedi & Neupane, 2024). In summary, Information Communication Technology serves as a fundamental pillar in modern accounting, driving efficiency, security, and innovation, but also requiring ongoing vigilance and adaptation to emerging challenges in the digital landscape.

2.2.2.1 Usage of Accounting Software

The usage of accounting software has fundamentally transformed the way organizations manage, record, and report financial transactions. As digitalization accelerates across the globe, accounting software now serves as the core operational tool for both large enterprises and small businesses, streamlining processes that were once heavily manual and prone to error. Contemporary accounting software offers a range of functionalities, from basic bookkeeping and automated ledger postings to sophisticated modules for tax management, fixed asset tracking, multi-currency accounting, and real-time financial

analysis (Rekhi & Johri, 2024). These features enable organizations to achieve higher levels of accuracy and efficiency, reducing the time required to close accounts, generate statements, and comply with regulatory requirements. One of the most significant advantages of accounting software is its ability to automate routine accounting tasks such as data entry, invoice processing, and reconciliation, which not only reduces human error but also liberates staff to focus on more strategic financial activities. Automated alerts and error-checking features built into modern software assist in identifying inconsistencies and anomalies at an early stage, thus supporting both internal controls and audit readiness (Ali et al., 2024). Integration with banking systems and other enterprise software, such as Enterprise Resource Planning (ERP) platforms, further ensures seamless data transfer across organizational functions, eliminating redundancies and enabling unified reporting (Mobilingo & Hailah, 2024).

Cloud-based accounting software has become particularly prevalent, providing organizations with real-time access to financial data regardless of geographical location. This accessibility supports remote work, enhances collaboration among finance teams, and allows for the timely review and approval of transactions by management. Data backup and disaster recovery features embedded in cloud systems offer an added layer of security, reducing the risk of data loss and supporting business continuity efforts (Rekhi & Johri, 2024). Additionally, many solutions now incorporate advanced analytics and dashboard

functionalities that enable decision-makers to visualize financial performance metrics instantly and identify trends or risks as they emerge (Ahmad et al., 2023).

Security is another critical consideration in the use of accounting software. Given the sensitive nature of financial data, leading software providers implement robust cybersecurity measures such as data encryption, multi-factor authentication, and user access controls. These features help protect against unauthorized access and data breaches, which are increasing in frequency and sophistication as cyber threats continue to evolve (Rathakrishnan & Baskar, 2024). Furthermore, accounting software supports compliance with statutory requirements by regularly updating tax codes, accounting standards, and reporting templates to reflect the latest regulatory changes (Ali et al., 2024). Importantly, the adoption of accounting software also plays a vital role in fraud prevention and detection. Automation minimizes the opportunity for manual manipulation of records, while audit trails created by the software log every transaction, change, or access event, making it easier to trace and investigate any suspicious activity (Werastuti et al., 2023). Machine learning and artificial intelligence capabilities are being embedded into some solutions to enable continuous monitoring of transactions, detect patterns indicative of fraud, and provide automated recommendations for further investigation (Adelakun et al., 2024). Training and user education are also critical to realizing the full benefits of accounting software. Organizations are increasingly recognizing the importance of equipping employees with the skills necessary to use these tools effectively and securely,

thereby reducing the risks associated with user errors and potential system misuse (Eghe-Ikhurhe et al., 2024). In summary, accounting software stands as a central pillar of modern financial management, driving operational efficiency, supporting regulatory compliance, strengthening internal controls, and playing an increasingly pivotal role in organizational risk management and fraud prevention.

2.2.2.2 Cybersecurity Measures

At the technical level, organizations implement advanced security protocols such as data encryption, firewalls, intrusion detection and prevention systems, and secure socket layer (SSL) certificates to protect the transmission and storage of sensitive accounting information. Encryption renders data unreadable to unauthorized users, even if accessed, while firewalls act as barriers to block malicious traffic and unauthorized system access. Intrusion detection and prevention systems continuously monitor networks for unusual activities or potential breaches, enabling swift responses to suspicious incidents. Secure authentication mechanisms, particularly multi-factor authentication (MFA), require users to provide multiple forms of verification before granting access, thereby reducing the risk of unauthorized entry even if passwords are compromised (Adelakun et al., 2024); (Mobilingo & Hailah, 2024).

Cybersecurity measures have become an indispensable aspect of modern accounting systems due to the exponential growth in the volume and sensitivity of financial data

processed digitally. With the proliferation of digital tools and interconnected accounting platforms, organizations face escalating threats from cybercriminals who target vulnerabilities for unauthorized access, data breaches, and fraud. In response, contemporary accounting environments prioritize robust cybersecurity frameworks designed to safeguard digital assets, ensure data integrity, and maintain stakeholder trust. These measures typically encompass technical, procedural, and human-centered approaches, forming a multi-layered defense against both external and internal threats (Rathakrishnan & Baskar, 2024).

Human-centered approaches are equally critical in the cybersecurity landscape. Employee ICT training and awareness programs ensure that users recognize threats such as phishing, social engineering, and malware, which often exploit human error rather than technological weaknesses. By fostering a culture of security, organizations empower staff to identify suspicious communications, adhere to safe password practices, and respond effectively to potential incidents (Eghe-Ikhurhe et al., 2024). Cybersecurity measures are integral to the trustworthiness and functionality of modern accounting systems. Their effectiveness hinges on a dynamic combination of advanced technology, stringent internal controls, regular monitoring, user education, and strategic policy implementation. As the digital environment continues to evolve, organizations must maintain a proactive approach, continuously adapting their cybersecurity posture to counter emerging threats and uphold the integrity of their financial information.

Procedurally, cybersecurity in accounting also involves the establishment and enforcement of internal controls, access rights, and segregation of duties. These controls are essential to limit system access to authorized personnel based on role and necessity, ensuring sensitive accounting data is not exposed to unnecessary risk. Regular system audits and compliance checks help organizations verify that security measures are functioning as intended and that any weaknesses are promptly addressed (Ali et al., 2024). Accounting software solutions often include audit trail features that record every transaction, system change, or data access event, enabling forensic reviews and supporting investigations into suspicious activities (Werastuti et al., 2023). The significance of cybersecurity measures in accounting extends beyond basic protection against unauthorized access. Effective cybersecurity frameworks also help maintain business continuity by safeguarding against ransomware, data loss, and service disruptions that could otherwise cripple financial operations. As accounting fraud schemes become more complex and technologically advanced, organizations increasingly rely on proactive monitoring and artificial intelligence to detect patterns indicative of fraud and to automate rapid responses to threats (Adelakun et al., 2024). Additionally, compliance with regulatory standards such as the General Data Protection Regulation (GDPR) or other national data protection laws is now a key aspect of organizational risk management, requiring continuous review and updating of cybersecurity strategies to reflect the evolving threat landscape (Rekhi & Johri, 2024).

2.2.2.3 Automated Internal Controls

Automated internal controls have become a cornerstone in the modern accounting environment, significantly enhancing the reliability, security, and efficiency of financial operations. With the rapid adoption of digital technologies and sophisticated accounting software, organizations are increasingly shifting from manual to automated internal controls to manage and safeguard their financial activities. Automated internal controls refer to system-driven checks and processes that are embedded within accounting and enterprise resource planning (ERP) systems, designed to ensure compliance, accuracy, and the prevention of fraud without constant human intervention (Ali et al., 2024). These controls function through mechanisms such as validation rules, approval workflows, segregation of duties, and real-time monitoring. For instance, validation rules programmed into accounting systems can automatically flag entries that fall outside predefined thresholds or fail to meet specific criteria, thereby preventing erroneous or suspicious transactions from being processed. Approval workflows ensure that transactions above a certain value or of a sensitive nature are reviewed by multiple authorized personnel before execution, reducing the risk of fraud and unauthorized activity (Werastuti et al., 2023). Automated segregation of duties prevents conflicts of interest by restricting the same individual from initiating, authorizing, and recording a transaction, a control that is essential for mitigating internal fraud risks.

The integration of artificial intelligence and machine learning further strengthens automated internal controls by enabling continuous transaction monitoring, anomaly detection, and pattern recognition. Advanced algorithms can analyze vast volumes of accounting data to identify unusual behaviors or trends indicative of fraud, error, or policy violations, often in real time. Such capabilities facilitate prompt investigation and corrective action, thereby minimizing financial loss and reputational damage (Adelakun et al., 2024). Another critical benefit of automated internal controls is the generation of comprehensive audit trails. Every transaction, modification, or access to financial data is automatically logged, providing a transparent and tamper-proof record that supports both internal audits and external regulatory requirements. This transparency not only deters fraudulent behavior but also expedites the audit process, making it easier to demonstrate compliance with laws and industry standards (Mobilingo & Hailah, 2024).

Automated controls also enhance operational efficiency by reducing the time and resources required for routine checks and reconciliations. For example, system-generated reconciliations of bank accounts, supplier statements, and customer balances can be performed more frequently and with greater accuracy than manual processes. This automation allows finance professionals to allocate more time to analytical and strategic functions, adding greater value to the organization (Rekhi & Johri, 2024). In the context of risk management, automated internal controls offer organizations a proactive defense against both internal and external threats. They continuously operate in the background,

adapting to new risks and regulatory requirements as system updates are deployed. The scalability and adaptability of these controls make them especially valuable for organizations experiencing rapid growth, increased transaction volumes, or heightened compliance obligations (Rathakrishnan & Baskar, 2024).

To maximize the effectiveness of automated internal controls, organizations must complement technology with regular reviews and updates to control configurations, user access rights, and system permissions. Employee training remains essential, ensuring that users understand how to operate within controlled environments and recognize system-generated warnings or alerts (Eghe-Ikhurhe et al., 2024). Automated internal controls are fundamental to maintaining the integrity, accuracy, and security of accounting information in the digital age. Their integration within modern accounting systems enables organizations to efficiently detect and prevent errors and fraud, comply with regulations, and support strategic decision-making through timely and reliable financial reporting.

2.2.2.4 Employee ICT training

Employee ICT training plays a pivotal role in ensuring the effective and secure use of information and communication technologies within accounting systems. As organizations increasingly rely on sophisticated digital tools for financial management, the competence of employees in using these technologies becomes a key determinant of both operational success and risk mitigation. Well-structured ICT training programs equip staff with the

necessary skills to operate accounting software, recognize potential cyber threats, adhere to internal controls, and respond appropriately to system alerts, thereby reducing the risk of errors, data breaches, and fraud (Eghe-Ikhurhe et al., 2024).

In the current digital landscape, cybercriminals frequently target the human element as the weakest link in organizational security. Even the most advanced cybersecurity systems and automated controls can be undermined if employees are unaware of how to spot phishing attempts, avoid unsafe behaviors, or follow secure password protocols. Research consistently highlights that ongoing employee ICT training is a critical defense against social engineering and cyberattacks, enabling staff to detect suspicious activities and take preventive action before vulnerabilities are exploited (Rathakrishnan & Baskar, 2024); (Adelakun et al., 2024). Furthermore, ICT training goes beyond basic digital literacy to include specialized instruction on the proper use of accounting systems, compliance with regulatory requirements, and adherence to organizational policies regarding data protection and internal controls. As accounting software and ERP systems become more advanced, training is necessary to ensure that employees can leverage the full capabilities of these tools such as automated reconciliations, real-time reporting, and advanced analytics without introducing unnecessary risk or inefficiency (Mobilingo & Hailah, 2024).

Effective employee ICT training programs are dynamic, adapting to technological advancements and emerging threats. They typically include regular updates and refresher sessions, 158 scenario-based learning, and practical exercises that simulate real-world

challenges. Organizations that invest in continuous training are better positioned to maintain a culture of security and accountability, foster compliance, and minimize human error within their financial processes (Rekhi & Johri, 2024).

In addition to strengthening technical skills, ICT training can raise awareness about the legal and ethical implications of digital conduct in accounting. By emphasizing the importance of confidentiality, data integrity, and ethical behavior, such training helps prevent both intentional misconduct and inadvertent policy violations (Eghe-Ikhurhe et al., 2024). Ultimately, employee ICT training is a vital component of any strategy aimed at leveraging technology in accounting, enhancing fraud prevention, and promoting organizational resilience. Its effectiveness is maximized when aligned with broader risk management practices and regularly evaluated to address new risks and opportunities arising from digital transformation.

Information Communication Technology and Accounting Fraud

The integration of Information Communication Technology (ICT) into accounting systems has significantly reshaped both the efficiency and the risks associated with financial management and reporting. While ICT enables faster data processing, real-time reporting, and improved accuracy in financial statements, it also opens new avenues for accounting fraud through sophisticated digital manipulation, system vulnerabilities, and weak internal controls. In recent years, researchers have increasingly focused on how ICT both aids and hinders efforts to combat accounting fraud. The use of ICT tools in forensic accounting has

shown promising results in speeding up investigations and improving the accuracy of evidence collection. For instance, a study in Nigeria confirmed that IT-based forensic accounting improves fraud detection speed and supports more accurate investigations, leading to better outcomes in legal contexts (Akinbowale & Esther, 2023). Artificial Intelligence (AI), as an extension of ICT, is also becoming instrumental in fraud prevention. A 2022 study in Indonesia found that AI-based Accounting Information Systems (AIS) have a significant positive impact on the detection and prevention of fraudulent financial reporting. The system's ability to process complex datasets and identify anomalies plays a major role in mitigating financial misconduct, with the study estimating a 71.7% effectiveness rate in fraud prevention (Meiryani et al., 2022).

Despite these benefits, ICT can also be exploited to carry out fraudulent activities. The automation and digital storage of accounting records create new cyber vulnerabilities. As companies increasingly rely on digital accounting systems, the risk of unauthorized access, data manipulation, and cyberattacks grows. Recent research has emphasized that safeguarding accounting information through cybersecurity measures such as encryption, access controls, and regular audits is essential to prevent fraudulent manipulation of financial data (Lehenchuk et al., 2022). Furthermore, legal frameworks are evolving to respond to these digital threats.

Accounting Software and Accounting Fraud

The rise of accounting software has revolutionized financial management across industries, enhancing efficiency, transparency, and data accuracy. However, it has also introduced new challenges related to accounting fraud. Recent research underscores the complex relationship between the use of accounting software and the prevalence of fraudulent financial activities, especially when software systems are misused or inadequately controlled. A 2023 study found that factors such as the efficiency, reliability, data quality, and ease of use of accounting software significantly affect the occurrence of fraud. The research shows that while accounting software is generally designed to enhance performance and reduce human error, poor implementation or misuse can still contribute to financial misconduct. Interestingly, the incorporation of artificial intelligence within accounting systems was noted to further improve organizational integrity and detection capabilities (Shuya Ma, 2023).

On a more technical front, forensic data analytics powered by machine learning and statistical modeling is emerging as a powerful method for detecting falsified financial reports. These tools analyze large datasets from accounting software to identify patterns typical of fraudulent behavior, offering targeted insights to auditors and regulators (Jofre & Gerlach, 2024). Accounting software is a double-edged sword in the fight against financial fraud. Its design and application can either serve as a safeguard against fraud or, if mismanaged, become a tool for concealment. To harness its full potential, organizations

must pair technological solutions with strong internal controls, training, and ethical standards.

Cybersecurity Measures and Accounting Fraud

Cybersecurity has become a critical line of defense against accounting fraud in today's digitized financial landscape. With the increasing use of Accounting Information Systems (AIS) and digital reporting tools, the threat of cyberattacks targeting financial data has intensified. This evolution has prompted researchers and organizations to explore how cybersecurity measures can prevent, detect, and respond to fraudulent financial activity. Recent studies underscore that multi-layered cybersecurity strategies incorporating technologies such as artificial intelligence, blockchain, and encryption are significantly improving data protection and fraud detection. For example, leading accounting firms like Deloitte and PwC have integrated such technologies into their systems to protect sensitive data, bolstering both client trust and audit integrity (Hasan et al., 2024).

Cybersecurity maturity, or the level of development and implementation of security frameworks, also plays a pivotal role in reducing accounting fraud risks. A 2025 study found that digital transformation initiatives when coupled with strong cybersecurity infrastructures significantly reduce fraud vulnerabilities within organizations (International Review of Management and Marketing, 2025). Strategic alignment between accounting and cybersecurity is increasingly recognized as essential. Integrating security protocols into accounting systems not only enhances financial data protection but also strengthens

stakeholder confidence. This synergy involves deploying encryption, AI-based analytics, and intrusion detection systems to prevent unauthorized data manipulation and financial fraud (Dawodu et al., 2023). In the context of tax accounting, a 2024 study emphasized that while tools such as multi-factor authentication and regular audits are effective, their inconsistent application especially among smaller firms creates significant vulnerabilities. Formal incident response plans and standardization of cybersecurity practices were identified as key gaps needing urgent attention (Nyombi et al., 2024).

Automated Internal Controls and Accounting Fraud

Automated internal controls are becoming essential tools in modern accounting systems to prevent and detect fraud. These controls, embedded within digital accounting platforms, function by enforcing consistent procedures, real-time monitoring, and immediate alerts for anomalies, thus reducing reliance on manual oversight and limiting opportunities for manipulation. Recent studies highlight that effective internal controls especially when automated significantly reduce the risk of accounting fraud by maintaining accuracy and accountability. A 2024 review found that robust internal control systems in public sector accounting are critical in preventing financial misreporting and fraud, with automation increasing both efficiency and reliability (Kesuma & Fachruzzaman, 2024). Similarly, another 2024 study emphasized that internal control frameworks directly impact the quality of accounting information and fraud reduction, especially when supported by consistent implementation and management commitment (Waromi et al., 2024).

However, the effectiveness of automated internal controls is not guaranteed unless the organizational environment supports ethical behavior and regulatory compliance. Research by Wardani and Nuraini (2023) showed that the presence of internal controls alone may not suffice unless accompanied by strict adherence to accounting rules and oversight. Their findings suggested that while internal control effectiveness alone had no significant effect on reducing fraud, compliance with accounting regulations played a decisive role (Wardani & Nuraini, 2023). Moreover, the interplay between automation and human factors remains a key consideration. Adiningrat (2022) observed that internal control structures, when coupled with values like spiritual accountability, can significantly improve fraud prevention. His research highlights the need to address not only technical implementations but also the ethical context in which controls operate (Adiningrat, 2022).

Employee ICT training and Accounting Fraud

Employee ICT training plays a crucial role in mitigating accounting fraud by improving employees' ability to detect, report, and prevent irregular financial activities. In today's digital environment, where financial systems are increasingly reliant on complex technology, organizations are recognizing that untrained staff can become inadvertent enablers of fraud due to their limited awareness of cybersecurity protocols, financial systems, and red flags associated with fraudulent behavior. A recent 2024 study found that forensic accounting training programs significantly strengthen banking sector resilience by equipping employees with fraud detection and prevention skills. These training programs

enhance professionals' investigative capabilities, awareness of fraud patterns, and adherence to regulatory standards, all of which contribute to more robust financial governance (Educational Administration Theory and Practices, 2024).

Although not focused exclusively on ICT, research by Brink et al. (2021) showed that internal audit functions used as management training grounds could affect how fraud is reported. Employees were more likely to report fraud when they perceived internal audit as trustworthy and independent. This finding implies that training must also cultivate organizational culture and ethical expectations to be fully effective (Brink et al., 2021). Finally, scholars have long argued that ICT-related skills are vital for auditors and accountants in today's risk-prone digital environment. An earlier review concluded that accountancy training institutions must embed ICT competencies in their curricula to ensure that financial professionals can navigate and audit complex systems without missing potential fraud indicators (Anomah & Agyabeng, 2013). Targeted ICT training for employees significantly enhances fraud detection and prevention in accounting. By integrating technical, analytical, and ethical components, training empowers employees to act as the first line of defense against fraudulent activity.

2.3 Theoretical Review

Fraud detection theories provide structured models for understanding the motivations, conditions, and systemic factors that lead to accounting fraud. These theories have evolved

over time in response to changing business environments, technological innovation, and increasingly complex fraud schemes.

2.3.1 Fraud Triangle Theory

The Fraud Triangle Theory, widely recognized as the foundational model for understanding occupational fraud, was developed by sociologist Donald Cressey in the early 1950s. Cressey's research into embezzlement and white-collar crime led him to identify three critical factors that must simultaneously exist for an individual to commit fraud: pressure, opportunity, and rationalization. Pressure refers to financial or personal stressors that drive individuals to seek illicit means of solving their problems, such as mounting debts, unmet financial goals, or job insecurity. Opportunity reflects the individual's perception of a low risk of detection and the presence of exploitable gaps in the organization's internal controls or oversight structures. Rationalization encompasses the cognitive justifications individuals use to legitimize their actions, such as a belief that they are merely "borrowing" the money or that their employer "owes" them due to perceived mistreatment (Ali et al., 2024); (Adekola et al., 2024).

The Fraud Triangle has provided the intellectual basis for decades of fraud risk assessment, audit methodology, and the design of internal controls. Auditors and organizational leaders are trained to identify signs of employee stress, design systems that minimize opportunities for fraud, and recognize rationalizing behaviors as early warning indicators. However, the

theory has faced several key criticisms. Most notably, it has been described as too simplistic for the modern business environment, focusing exclusively on individual motivations and ignoring broader organizational, cultural, or technological influences (Judijanto & Defitri, 2024). The Fraud Triangle also fails to address collusion or the role of management override in enabling fraud. Despite these criticisms, its simplicity and clarity make it an enduring foundation for understanding and teaching basic fraud risk concepts, and it continues to inform best practices in fraud prevention worldwide.

and it continues to inform best practices in fraud prevention worldwide.

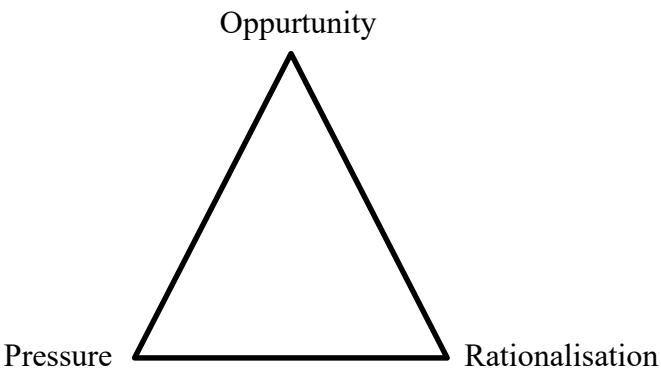


Fig. 2.1: Fraud Triangle Theory

2.3.2 Fraud Diamond Theory

In 2004, David T. Wolfe and Dana R. Hermanson advanced fraud theory by introducing the Fraud Diamond. Recognizing the limitations of the Fraud Triangle, they added a fourth dimension: capability. According to the Fraud Diamond Theory, fraud cannot occur unless

the perpetrator not only faces pressure, perceives opportunity, and can rationalize the behavior, but also possesses the capability to recognize, exploit, and conceal the fraud. This includes specific skills, access, intelligence, confidence, and even the ability to deal with stress and avoid detection. Capability explains why, within organizations, some individuals are more likely than others to perpetrate complex and sustained frauds particularly those who hold senior positions, have deep knowledge of internal systems, or can override controls (Werastuti et al., 2023).

The Fraud Diamond has had a substantial impact on both the academic and practical aspects of fraud risk management. Organizations now pay closer attention to "red flag" employees who not only have motive and opportunity but also possess a unique capability to commit and conceal fraud. Pre-employment screening, rotation of duties, and succession planning all incorporate considerations of capability. Nonetheless, the Fraud Diamond is not without its detractors. Critics contend that while the addition of capability brings valuable nuance, the theory remains individual-centric and does not adequately address system-wide or environmental factors such as organizational culture, ethical climate, or the enabling role of technology (Ali et al., 2024). Furthermore, capability is sometimes difficult to measure objectively, making its operationalization in fraud prevention programs challenging.

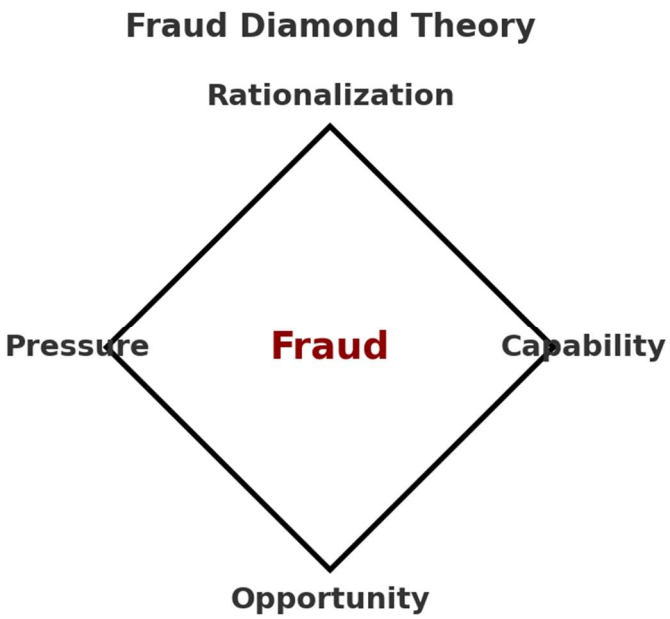


Fig 2.2: Fraud Diamond Theory

2.3.3 Fraud Pentagon Theory

To address emerging criticisms and further broaden the understanding of fraud perpetration, Jonathan Mark introduced the Fraud Pentagon Theory in 2010. This model retains the core elements of the Fraud Triangle (pressure, opportunity, and rationalization) and the Fraud Diamond's capability, but adds a fifth dimension: arrogance. Arrogance refers to a sense of superiority or entitlement that leads individuals often in powerful positions to believe that organizational rules and controls do not apply to them. This element is especially relevant for top management or executives who may override established controls or manipulate financial statements with impunity. Competence is also

further emphasized in this theory, focusing on both the technical ability to commit fraud and the intellectual sophistication to plan and execute complex schemes (Adekola et al., 2024).

The Fraud Pentagon Theory has proven particularly useful in forensic investigations of large-scale corporate frauds, where personality traits such as arrogance, hubris, or a lack of ethical restraint are often major contributing factors. Organizations adopting this theory incorporate behavioral risk indicators into their fraud prevention strategies and whistleblower programs, with enhanced vigilance towards those in authority who exhibit such traits. Despite its contributions, the Fraud Pentagon has also been critiqued. Its behavioral dimensions, like arrogance and competence, can be difficult to assess reliably and may introduce subjectivity into risk assessments (Judijanto & Defitri, 2024). In rapidly digitizing environments, it may still fall short in addressing technological vulnerabilities, complex organizational structures, and external threats such as cybercrime.

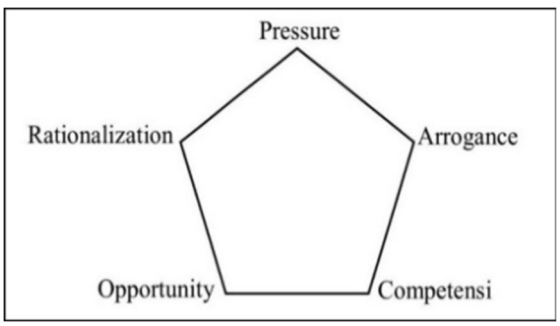


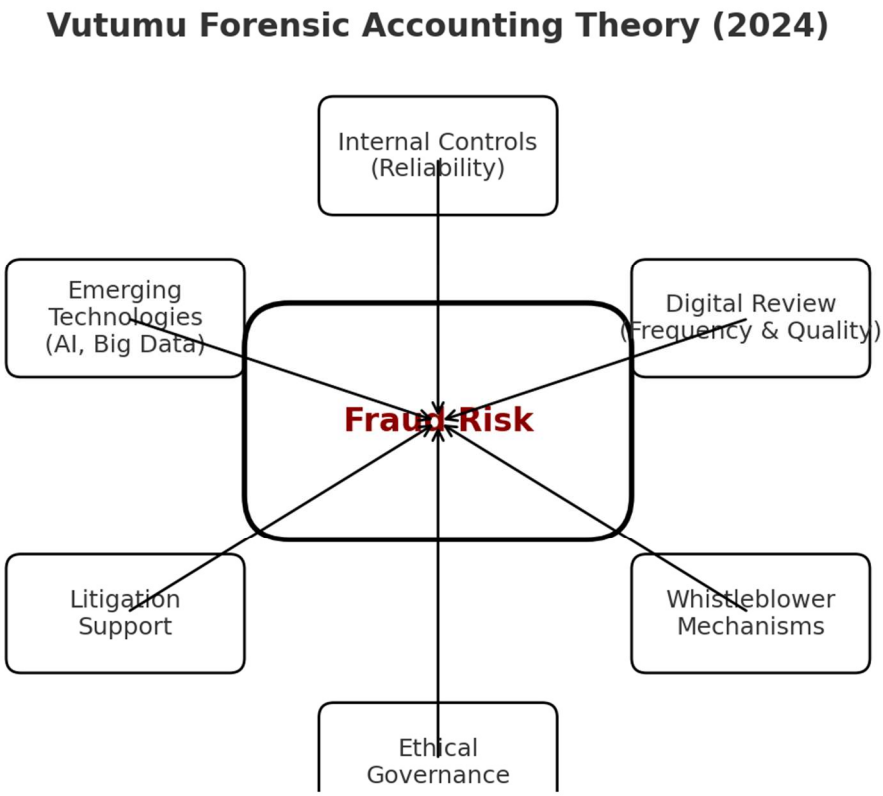
Fig 2.3: Fraud Pentagon Theory

2.3.4 Vutumu Forensic Accounting Theory (2024)

The Vutumu Forensic Accounting Theory, proposed by Aloysius Vutumu in 2024, represents the latest and most integrated approach to understanding and combating accounting fraud. This theory synthesizes decades of fraud research and responds directly to the complexities introduced by globalization, technological innovation, regulatory shifts, and digital transformation in accounting practices. Unlike previous theories, the Vutumu framework recognizes that fraud cannot be understood solely through the lens of individual motivations or behavioral traits; rather, it emerges from a dynamic interplay of individual, organizational, technological, regulatory, and cultural factors (Vutumu, 2024).

Central to the Vutumu Theory are several interlocking components: reliability of internal control systems, frequency and quality of digital system reviews, the presence of whistleblower mechanisms, integration of ethical governance, strength of litigation support, and proactive adoption of emerging technologies in audit and fraud detection. The theory explicitly addresses the role of information and communication technology (ICT) by including digital fraud review frequencies, automated monitoring, and the integration of artificial intelligence and big data analytics as primary deterrents and detection mechanisms for fraud. It emphasizes that effective fraud prevention is rooted in robust,

continually updated internal controls, ongoing employee ICT training, transparent and responsive governance, and a culture of accountability (Vutumu, 2024).



2.3.5 Theoretical Framework

This study underpins itself on the Vutumu Theory because it aligns perfectly with the research focus on the impact of ICT tools (such as accounting software, ERP systems,

cybersecurity, and employee ICT training) on fraud detection and prevention. Unlike older theories, Vutumu's framework encompasses not only personal and behavioral factors but also systemic and technological influences, making it especially relevant for organizations navigating the complexities of digital accounting environments. The Vutumu Theory supports a holistic analysis incorporating organizational structure, compliance culture, digital readiness, and external regulatory frameworks necessary to understand and combat contemporary accounting fraud (Vutumu, 2024).

Critics of the Vutumu Theory argue that its comprehensive scope can be difficult to implement, especially for small and medium enterprises lacking the resources for sophisticated digital tools, regular audits, and continuous training. Some suggest that the theory's broadness may dilute focus and complicate the identification of key fraud risk indicators in practice (Vutumu, 2024). However, these criticisms are outweighed by the necessity for an adaptable, integrated approach in today's fast-evolving technological and regulatory landscape. The Vutumu Theory stands out as the most perfect underpinning framework for this study because it uniquely integrates all facets technological, human, organizational, and regulatory necessary to fully address the multifaceted nature of accounting fraud in the digital age.

2.4 Empirical Review

Gomez (2025) investigated the impact of forensic accounting skills, particularly those enhanced by ICT training, on the self-efficacy of fraud detection among social security account officers in the Philippines. The study aimed to assess which specific skills contribute most to an individual's confidence and effectiveness in identifying fraudulent activities, with a focus on the influence of psycho-social and communication skills derived from ICT-enabled learning environments. The methodology involved a descriptive-correlational survey, where data were gathered using a researcher-developed questionnaire validated through pilot testing. Respondents included account officers from three Philippine regions: Central Luzon (Region III), CALABARZON (Region IV-A), and MIMAROPA (Region IV-B). The study did not specify the total number of participants but ensured representativeness by covering multiple regions. Data analysis was conducted using descriptive statistics and regression analysis to determine the impact of various skill sets on fraud detection self-efficacy. Key findings indicate that account officers possessed advanced proficiency in a range of forensic accounting skills, with psycho-social skills showing a significant positive effect on self-efficacy in fraud detection. Communication skills also played a role, though interestingly, the effect was negative suggesting possible complexities or overconfidence issues. Technical, analytical, accounting, and auditing skills, although important, did not have a statistically significant impact on self-efficacy according to the regression results. Based on these insights, the study proposes a competency development plan that emphasizes psycho-social and communication skills as critical areas for training and professional development. The main gap highlighted by

Gomez is the limited focus on the evaluation of accounting software and automated internal control measures, which are also vital components of effective fraud detection in the ICT era. The study underscores the need for future research to explore the integration of these technological tools and to empirically assess their specific impact on fraud detection outcomes, beyond the scope of individual skillsets (Gomez, 2025).

Adelakun et al. (2024) conducted a comprehensive review to explore how artificial intelligence (AI) is transforming fraud detection practices in the accounting sector. The primary objective of the study was to provide an overview of the latest AI-driven techniques and to highlight their effectiveness compared to traditional fraud detection approaches. The authors specifically focused on the integration of machine learning (ML), natural language processing (NLP), and data mining within accounting systems, analyzing their ability to detect complex fraud patterns that conventional systems may miss. Methodologically, the paper adopts a review and case study approach. The authors synthesize existing literature and examine real-world instances where AI technologies have been deployed to detect fraud in financial transactions. Although the study does not specify a particular sample size or confine itself to a particular country, it draws examples from global financial institutions and multinational corporations, providing a broad perspective on the issue. The findings indicate that AI-powered tools, especially those employing ML algorithms, significantly enhance the ability to identify and prevent fraudulent transactions in real-time. For instance, machine learning models can analyze vast quantities of

transaction data, flagging anomalies that deviate from established norms. NLP, meanwhile, is highlighted as an effective tool for analyzing unstructured textual data, such as financial documents and internal communications, thereby uncovering hidden fraud schemes. Case studies illustrate that the implementation of AI has led to the detection of sophisticated fraud that had previously gone unnoticed, and has allowed organizations to respond more swiftly and effectively to emerging threats. Despite these advancements, the study acknowledges several limitations. The most notable gap is the lack of large-scale quantitative empirical testing to substantiate the efficacy of AI methods across diverse settings. Most evidence is drawn from illustrative cases rather than systematic analysis. Furthermore, the paper suggests that future research should focus on empirically validating these techniques and exploring their scalability and adaptability in different organizational and regulatory contexts. In conclusion, while AI offers promising improvements in fraud detection within accounting, a need remains for rigorous empirical studies to fully assess its impact (Adelakun et al., 2024).

Djuharni et al. (2024) set out to investigate the intricate relationships between law enforcement and auditors in the context of accounting fraud detection and prevention. The objective of the study was to synthesize current knowledge on how these two professional groups interact, coordinate, and influence the broader landscape of fraud mitigation. The authors were particularly interested in the roles, responses, and the sometimes complicated dynamics that arise between auditors and law enforcement agencies. The methodology

employed was a mixed methods review, focusing on journal articles published between 2014 and 2024. The authors utilized keywords such as “Auditors,” “Enforcement,” “Accounting fraud,” “responses,” and “complicated relationships” to guide their systematic literature review. Data collection was facilitated through research databases including SINTA, Semantic Scholar, and Google Scholar, employing tools such as Publish or Perish (PoP) and SLR 7P to ensure a comprehensive literature search. The study, however, did not specify a sample size in terms of reviewed articles, nor did it confine its analysis to a particular geographical region, thus providing a global perspective. The main findings highlight that effective coordination and information sharing between auditors and law enforcement are crucial to detecting and addressing accounting fraud. The review reveals that while advances in corporate monitoring systems have been made, significant cases of accounting fraud persist even in robust institutional environments, underscoring the need for stronger auditor-law enforcement collaboration. The literature also points out the influence of law enforcement actions on auditor-client relationships and the willingness of clients to disclose relevant information, which can be both a facilitator and a barrier to effective fraud detection. A key gap identified by the authors is the limited availability of empirical case studies that directly examine the interplay between auditors and law enforcement in real-world fraud investigations. Most of the existing literature is conceptual or descriptive, lacking detailed accounts of practical coordination efforts or measurable outcomes. Djuharni et al. call for more in-depth, empirical research focusing on case studies that can illuminate best practices and challenges in these professional interactions.

Such work would be invaluable in informing both academic understanding and practical strategies for fraud prevention (Djuharni et al., 2024).

Ali et al. (2024) examined the impact of emerging technologies specifically artificial intelligence (AI), blockchain, and data analytics on forensic accounting practices and the effectiveness of fraud detection. The objective of their study was to empirically assess whether these technological advancements contribute to more efficient and effective identification and prevention of fraud compared to previous traditional methods. The authors employed a robust methodological framework, which included regression analysis, the Beneish M-Score, and Benford's Law. Their empirical analysis encompassed 100 companies for the regression models assessing the effectiveness of forensic accounting, and a separate sample of 50 companies for testing the impact of blockchain technology on transparency and fraud detection. The study does not specify the geographical locations of the companies included, suggesting a broad or multi-regional scope. Findings from the regression analysis indicate that both data analytics (with a coefficient of β=0.35) and AI (β=0.30) exert a substantial positive effect on enhancing fraud detection efficiency. The application of blockchain technology among firms with high transaction volumes was also found to significantly improve transparency and traceability, which in turn facilitated better fraud detection. Moreover, the use of the Beneish M-Score allowed for the identification of multiple companies potentially engaged in earnings manipulation, further supporting the value of advanced forensic techniques. These results collectively affirm that technological

integration in forensic accounting leads to significant improvements in the detection and prevention of fraudulent activities. Despite these positive outcomes, Ali et al. acknowledge notable limitations in their study. A primary gap is the need for further research into the scalability of these technologies, particularly in terms of their long-term effectiveness and applicability across different sectors and organizational contexts. Additionally, successful implementation of advanced forensic tools requires significant investment in infrastructure and staff training, which may not be feasible for all organizations. The authors recommend that future research should focus on evaluating the practical challenges of widespread adoption and the potential for long-term integration of these technologies in forensic accounting (Ali et al., 2024).

Baldini (2023) focused on the legislative and regulatory aspects influencing accounting fraud in Italy, following significant reforms aimed at strengthening corporate internal controls and enhancing the authenticity of accounting information. The objective was to analyze the effects of Italy's Law No. 69/2015, which was introduced to restore and fortify penalties against the crime of false corporate communications a common form of accounting fraud. Using a descriptive legal analysis methodology, the paper systematically reviewed the changes in Italian law and compared the new regulations with the previous legal framework. The study did not specify a sample size, as it was not empirical but rather a comprehensive review of legal texts, regulatory updates, and secondary literature. The analysis was geographically limited to Italy, offering in-depth insights into the country's

regulatory environment. The findings reveal that the strengthened regulations have contributed to an improvement in the quality of accounting information and, by extension, fraud detection and prevention. The new legal provisions emphasize the necessity of robust internal controls and impose stricter penalties for misrepresentation and manipulation of financial statements. These measures, according to Baldini, have heightened awareness among corporate managers and fraud examiners regarding the areas most susceptible to fraudulent activities. Additionally, the study underscores the role of modern technological tools and information systems in supporting compliance and internal control mechanisms. A key gap identified in this research is its descriptive nature; it does not empirically test the direct impact of information and communication technology (ICT) on the occurrence or detection of accounting fraud. While the regulatory reforms discussed provide a foundation for improved fraud mitigation, the paper does not present data-driven evidence regarding the effectiveness of specific ICT tools or automated internal controls in practice. Baldini suggests that future research should focus on empirical evaluations that link technological adoption to fraud outcomes, thereby providing a clearer picture of ICT's role in accounting fraud prevention (Baldini, 2023).

Cyril et al. (2023) conducted an empirical study to assess the effect of information and communication technology (ICT) on accounting practices in Nigeria, with a particular focus on the efficiency and reliability of accounting processes and their implications for fraud prevention. The objective was to determine whether the adoption of ICT leads to

improved efficiency and timeliness in accounting operations, and to evaluate its broader impact on fraud prevention within organizational settings. The study employed a quantitative survey methodology, utilizing a structured questionnaire based on a five-point Likert scale to gather data from accounting professionals in Nigeria. Statistical analysis was performed using ANOVA with the aid of SPSS software to test the formulated hypotheses. While the exact sample size is not specified in the summary, the research context is clearly set within the Nigerian business environment. Findings from the study demonstrate that the adoption of ICT has a positive effect on the efficiency and timely delivery of accounting services. Respondents reported that ICT tools streamline accounting tasks, facilitate real-time processing, and help ensure the accuracy of financial records. Importantly, the results suggest that ICT adoption contributes to the prevention of accounting fraud by enabling better monitoring, quicker detection of irregularities, and more robust data security protocols. The study recommends that organizations fully integrate ICT across all accounting operations and invest in continuous training to maximize these benefits. Despite these encouraging findings, a notable limitation is the study's failure to separately and systematically measure the impact of ICT on specific fraud detection mechanisms. The research primarily addresses overall accounting efficiency and general fraud prevention, without isolating the effects of particular technologies (such as encryption, automated controls, or cybersecurity measures) on fraud outcomes. Cyril et al. call for future studies that focus more narrowly on the direct relationship between distinct ICT tools and the incidence or detection of accounting fraud (Cyril et al., 2023).

Wamukota et al. (2022) examined the effect of accounting information and communication control systems, key aspects of ICT infrastructure, on the financial performance and fraud risk of savings and credit cooperative organizations (SACCOs) in Kenya. The objective was to empirically determine whether robust accounting information systems are linked to improved financial outcomes and a reduction in fraud incidences. The study adopted a mixed-methods design, combining survey data with secondary analysis of audited financial statements. The target population comprised 175 SACCOs across Kenya, involving 875 respondents including CEOs, finance managers, risk managers, ICT managers, and internal auditors. Data collection utilized questionnaires for primary data and document analysis for secondary data. Statistical tools included regression analysis to establish relationships between variables. The findings demonstrated a significant positive correlation between the quality of accounting information and communication control systems and the financial performance of SACCOs. More specifically, the study found that effective control systems supported by ICT were associated with reduced fraud risk and better overall organizational performance. Accounting information and communication controls explained 43.7% of the variance in financial performance, underscoring the critical role of ICT in modern financial management and fraud prevention. However, the authors note several gaps in their work. While the study confirms the broad effectiveness of accounting information systems, it does not isolate or evaluate the impact of specific cybersecurity measures, such as encryption or multi-factor authentication, which are increasingly important in combating digital fraud. The authors recommend that future research should focus on dissecting the

relative effectiveness of individual ICT controls and their direct impact on fraud detection and prevention (Wamukota et al., 2022).

Ali and Handro (2022) explored the perceptions of accountants and auditors regarding the use of technology and integrity as means for preventing accounting fraud. The objective was to determine whether there is a consensus among accounting professionals about which technological tools and personal attributes are most effective in fraud prevention. The study utilized a quantitative survey methodology, distributing questionnaires to 110 accounting alumni of Riau Caltex Polytechnic who graduated between 2015 and 2019 and were employed as accountants or auditors in Indonesia. The data were analyzed using independent sample t-tests to identify differences in perceptions between the two professional groups. The results show that both accountants and auditors generally agree on the importance of technology in preventing fraud, particularly measures such as anti-virus software and surveillance cameras (CCTV). Both groups also highlighted the importance of maintaining high standards of integrity as a core personal attribute in fraud prevention. Notably, while there were some differences in the preference for specific technological tools, the overarching view was that the integration of technology and ethical conduct are both critical in minimizing fraud risks. Despite the positive findings, the study has certain limitations. Specifically, it does not explore the effectiveness of advanced ICT security measures such as encryption or multi-factor authentication, focusing instead on more general tools and broad concepts of integrity. The research is also limited by its

sample size and geographic focus. The authors suggest that future research should assess the effectiveness of specific cybersecurity technologies in various organizational contexts and examine their integration with ethical training for accounting professionals (Ali & Handro, 2022).

Martins and Francisco (2021) conducted a study to assess the impact of information and communication technology (ICT) on the practices of certified accountants, with a focus on the perceptions of professionals regarding how technological adoption influences the quality and efficiency of accounting work. The primary objective was to understand the perceived benefits and drawbacks of ICT in the accounting profession, as well as its implications for fraud detection and prevention. The researchers used a survey methodology, targeting certified accountants in the Leiria district of Portugal. The survey explored various dimensions of ICT use, including its effects on data processing speed, information accuracy, and overall reliability of financial reporting. Although the exact sample size is not specified, the study's findings are based on the aggregated responses of practicing accountants in the region. Results from the survey indicate that the adoption of ICT is widely recognized as fundamental to modern accounting practice. Respondents noted significant improvements in the speed and efficiency of data collection and processing, as well as the quality and reliability of the information produced. These advancements are credited with reducing the time needed to complete accounting tasks and with supporting more effective detection and prevention of fraud. However, the study also

points out that some accountants still face challenges adapting to new technologies, and that ongoing training is necessary to maximize the benefits of ICT. A notable gap in this research is the focus on professionals' perceptions rather than on empirical fraud statistics or direct measurements of fraud outcomes. While the study establishes a positive link between ICT adoption and improved accounting practices, it does not provide quantitative evidence on the extent to which ICT reduces fraud incidents. The authors recommend future research that goes beyond perceptions to empirically measure the impact of specific ICT tools on the actual detection and prevention of accounting fraud (Martins & Francisco, 2021).

Table 2.1: Summary of Empirical Review

S/N	Author Name and Date	Title	Methodology	Sample Size	Location	Findings	Gaps
	Beatrice Oyinkansola Adelakun et al., 2024	Enhancing fraud detection in accounting through AI: Techniques and case studies	Review and case studies	Not specified	Not specified	AI (ML, NLP, data mining) greatly improves fraud detection compared to traditional methods.	Lacks quantitative empirical testing; focuses on illustrative cases. (Adelakun et al., 2024)
	Darti Djuharni et al., 2024	Law enforcement and auditors' roles, responses, and complicated relationships in accounting fraud	Mixed methods review of 2014–2024 articles	Not specified	Not specified	Strong coordination between auditors and law enforcement is vital to detecting and mitigating fraud.	Suggests need for more empirical case studies on auditor-law enforcement collaboration. (Djuharni et al., 2024)

	Ahmed Mustafa Ali et al., 2024	Forensic Accounting and Fraud Detection Emerging Trends and Techniques	Regression analysis, Beneish M-Score, Benford's Law	100 (regression), 50 (blockchain test)	Not specified	AI, blockchain, and data analytics significantly enhance fraud detection; blockchain improves transparency.	Further research needed on scalability and long-term application in diverse contexts. (Ali et al., 2024)
	M. Baldini, 2023	Risks of false accounting: Some reflections on the new regulation in Italy	Descriptive legal analysis	Not specified	Italy	Strengthened regulation improves accounting information quality and fraud detection; emphasizes need for strong internal control.	Descriptive; does not empirically test ICT's direct impact. (Baldini, 2023)
	Prof. Ubesie Madubuko Cyril et al., 2023	Effect of Information and Communication Technology (ICT) on Accounting Practice in Nigeria	Survey, Likert scale, ANOVA	Not specified	Nigeria	ICT adoption improves accounting efficiency and fraud prevention in practice.	Did not separately measure effect on fraud detection mechanisms. (Cyril et al., 2023)
	Adrian M. Gomez, 2025	Forensic Accounting Skills as Determinants of Self-Efficacy in Fraud Detection	Descriptive-correlational survey, regression	Not specified	Philippines	Psycho-social and communication skills from ICT-related training improve self-efficacy in fraud detection.	Does not evaluate software or internal control measures. (Gomez, 2025)
	José Luís Pereira Martins & Tiago Miguel Moniz	The impact of using ICT in the practice of certified accountants	Survey of certified accountants	Not specified	Portugal	ICT increases efficiency, quality, and reliability of accounting; supports fraud	Focuses on perceptions; no fraud statistics measured. (Martins & Francisco, 2021)

	Francisco, 2021					detection and prevention.	
	Mackline Wamukota et al., 2022	Effect of accounting information and communication control on financial performance of Sacco's in Kenya	Mixed design: survey + secondary data	175 SACCOs, 875 respondents	Kenya	Significant positive relationship between accounting information/control systems (ICT) and financial performance (fraud reduction).	Does not isolate cyber controls' effect; focuses broadly on information systems. (Wamukota et al., 2022)
	Fifitri Ali & Alex Handro, 2022	Accountants and auditors' perceptions of technology and attitude of integrity in preventing fraud	Survey, t-test	110 accountants/auditors	Indonesia	Accountants and auditors recognize technology (anti-virus, CCTV) and integrity as effective for fraud prevention.	Specific ICT measures like encryption/MFA not studied; focus is broader. (Ali & Handro, 2022)

Source: Author's Compilation, 2025.

2.5 Gaps in Literature

The literature reveals several gaps in the existing research on fraud detection and prevention within the accounting sector, particularly concerning the role of emerging technologies and professional interactions. While numerous studies highlight the

promising applications of artificial intelligence (AI), blockchain, data analytics, and information and communication technology (ICT), there is a notable absence of large-scale empirical testing to substantiate the effectiveness of these technologies across various contexts. For instance, although AI-driven tools, such as machine learning (ML) and natural language processing (NLP), have demonstrated improvements in fraud detection, many studies primarily rely on case studies rather than systematic empirical evidence (Adelakun et al., 2024). Similarly, studies that focus on forensic accounting, such as Ali et al. (2024), affirm the positive effects of AI and data analytics in enhancing fraud detection, yet they emphasize the need for further research on the scalability and long-term impact of these technologies. Furthermore, there is a shortage of empirical research examining the practical coordination between auditors and law enforcement, with most studies being either conceptual or descriptive (Djuharni et al., 2024). This gap limits the understanding of the real-world dynamics that could strengthen fraud mitigation strategies.

Additionally, while studies like those of Cyril et al. (2023) and Wamukota et al. (2022) underscore the role of ICT in improving efficiency and fraud prevention, they do not isolate the impact of specific technological tools, such as encryption or automated internal controls, on fraud outcomes. The lack of detailed investigation into the effectiveness of these individual tools means that the literature overlooks the specific mechanisms through which ICT influences fraud detection and prevention. Moreover, although studies have highlighted the positive impact of regulatory reforms, such as those in Italy (Baldini, 2023),

on fraud detection, there is a dearth of empirical studies linking technological adoption to concrete outcomes in fraud reduction.

Another critical gap is the limited focus on the integration of psycho-social and communication skills in fraud detection, as suggested by Gomez (2025). While such skills have been identified as important for self-efficacy in detecting fraud, there is a lack of research into how ICT-enhanced training programs might improve the effectiveness of these skills. Similarly, the role of ICT in supporting auditor-client relationships and enhancing communication between auditors and law enforcement remains underexplored, despite its importance in combating fraud. Finally, the studies point to a general lack of quantitative research that links ICT competencies in accounting education to actual reductions in fraud. As Daff (2021) notes, while ICT and software skills are deemed crucial by employers, the connection between these skills and measurable improvements in fraud detection is largely untested.

In conclusion, while there is considerable theoretical support for the role of advanced technologies in fraud detection and prevention, the literature still lacks rigorous empirical evidence on the long-term scalability, practical implementation, and specific impacts of these technologies in diverse organizational and regulatory contexts. Future research should focus on conducting large-scale, quantitative studies to fill these gaps and provide more concrete insights into the effectiveness of ICT tools and professional collaborations in fraud prevention.

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This chapter outlines the research methodology adopted for investigating the impact of Information Communication Technology (ICT) on accounting fraud in selected private firms in Benin City, Edo State. It provides a detailed description of the research design, population, sample size, and sampling techniques used in the study. Additionally, it highlights the data collection instruments, which include a structured questionnaire designed to gather relevant data from respondents. The chapter also discusses the methods for data analysis, specifically the techniques used to evaluate the relationship between ICT components and the prevalence of accounting fraud.

3.2 Research Design

This study adopted a descriptive survey design to examine the impact of ICT tools on accounting fraud in selected private firms in Benin City. The descriptive approach was chosen because it allows the researcher to systematically describe and analyze the relationship between various ICT components (such as accounting software, cybersecurity measures, internal control automation, and employee ICT training) and accounting fraud.

3.3 Population of the Study

The population of the study comprised finance-related employees, including accountants, auditors, and IT personnel, in selected private organizations within Benin City, Edo State. The population included staff involved in accounting operations, fraud detection, and ICT deployment to ensure a comprehensive understanding of the subject matter.

3.4 Sample Size and Sampling Technique

The sample size for this study was determined using the Cochran formula for infinite populations. Given that the population size of accountants, auditors, and IT personnel is unknown, the Cochran formula is the most appropriate and standard method for calculating sample size. The formula is as follows:

$$n_o = \frac{Z^2 \cdot \mathbf{p} \cdot (\mathbf{1}-\mathbf{p})}{e^2}$$

where;

n_0 is the sample size needed.

Z is the Z-value corresponding to the desired confidence level.

p is the estimated proportion of the population that exhibits the characteristic of interest.

e is the margin of error.

substituting the values;

Z = 1.96 (for 95% confidence level)
p = 0.5 (estimated proportion)
e = 0.05 (5% margin of error)

therefore;

$$n_o = \frac{1.96^2 \cdot \mathbf{0.5} \cdot (\mathbf{1} - \mathbf{0.5})}{0.05^2}$$

$$= \frac{3.84 \text{ x } \mathbf{0.5} \text{ x } (\mathbf{0.5})}{0.0025}$$

$$= \frac{0.96}{0.0025}$$

$$= 384$$

Thus, the sample size required for this study is 384 respondents. This ensures that the sample is large enough to provide valid and reliable results. A convenience sampling technique was used to select participants for this study. Convenience sampling involves selecting respondents who are readily accessible and willing to participate. Although this sampling method may introduce some bias, it was deemed appropriate for the study given the time and resource constraints.

3.5 Operationalization of Variables

The variables in this study were operationalized using a 5-point Likert scale to measure respondents' perceptions. Table 3.1 below outlines the operationalization of variables:

Variable	Definition	Indicators	Measurement Scale
Accounting Software (AS)	Use of digital tools to record, track, and report finances.	Accuracy, automation, accessibility	1 = Strongly Disagree to 5 = Strongly Agree
Cybersecurity Measures (CS)	ICT tools for protecting accounting systems from breaches.	Firewalls, password protection, access control	1 = Strongly Disagree to 5 = Strongly Agree
Internal Control Systems (IC)	Computerized checks that detect and prevent fraud.	Automation, reliability, real-time alerts	1 = Strongly Disagree to 5 = Strongly Agree
Employee ICT Training (ET)	Formal training for accounting and system users.	Frequency, relevance, effectiveness	1 = Strongly Disagree to 5 = Strongly Agree
Accounting Fraud (AF)	The manipulation or misrepresentation of financial data.	Incidence, detection rate, financial loss	1 = Strongly Disagree to 5 = Strongly Agree

3.6 Data Collection Methods

The study utilized primary data collected through structured questionnaires. The questionnaire was divided into two sections: Section A focused on demographic information such as age, gender, educational background, job position, and years of

experience. Section B addressed variables related to ICT tools, such as accounting software, cybersecurity, internal controls, ICT training, and accounting fraud.

3.7 Validity and Reliability of the Instrument

The questionnaire was reviewed by experts in information systems and accounting to ensure content and face validity. A pilot test was conducted with 10 professionals from firms outside the main study area, and necessary adjustments were made based on their feedback. The reliability of the questionnaire was tested using Cronbach's Alpha. A coefficient value of 0.7 and above was considered acceptable for internal consistency of the instrument.

3.8 Model Specification

The relationship between ICT components and accounting fraud was specified using a multiple regression model as follows:

$$AF = \beta_0 + \beta_1 AS + \beta_2 CS + \beta_3 IC + \beta_4 ET + \varepsilon$$

Where:

- AF = Accounting Fraud (dependent variable)
- AS = Accounting Software
- CS = Cybersecurity Measures
- IC = Internal Control Systems
- ET = Employee ICT Training

- β_0 = Intercept
- β_1–β_4 = Coefficients of the independent variables
- ε = Error term

3.8 Method of Data Analysis

The data collected was analyzed using both descriptive and inferential statistical techniques: Descriptive statistics such as frequency, mean, and standard deviation were used to summarize respondents' demographic characteristics and their responses to ICT-related variables. Inferential statistics including Pearson correlation and multiple regression analysis were used to test the research hypotheses and determine the strength and direction of the relationships between ICT tools and accounting fraud. The analysis was conducted using the Statistical Package for the Social Sciences (SPSS), with a 5% level of significance ($p < 0.05$).

CHAPTER FOUR

PRESENTATION OF RESULTS AND DISCUSSION OF FINDINGS

4.0 Introduction

This chapter presents the results of the findings, interprets and discusses the findings of the study. 384 copies of the questionnaires were administered to the respondents and 380 copies were retrieved, valid and used for the analysis.

4.2 Presentation of Result

The data collected were summarized and presented in the tables below. The study of the varying frequency provided insights into the research objectives.

Table 4.1 Demographic Representation

Gender	**Number of Respondents**	**Percentage**
Female	151	39.7
Male	229	60.3
Total	**380**	**100.0**
18 - 25	18	4.7
26 -35	211	55.5
36 -45	123	32.4
46 and Above	28	7.4
Total	**380**	**100.0**

Educational Qualification	**Frequency**	**Percentage**
HND/Bsc	224	58.9
Msc/MBA	110	28.9
OND	23	6.1
PhD	23	6.1
Total	**380**	**100.0**
Current Position	**Frequency**	**Percentage**
Accountant	122	32.1
Auditor	24	6.3
Finance Officer	120	31.6
IT Personnel	114	30.0
Total	**380**	**100.0**
Years of Work Experience	**Frequency**	**Percentage**
2 - 5 years	212	55.8
6- 10 Years	124	32.6
Above 10 years	23	6.1
Less than 2 years	21	5.5
Total	**380**	**100.0**

Source: Field Survey, (2025)

The demographic profile of the 380 respondents reveals a male majority (60.3%) and a predominant age range of 26–35 years (55.5%), suggesting a relatively young and professionally active sample. Educationally, most participants hold an HND or BSc (58.9%), with a notable proportion (28.9%) having postgraduate qualifications (MSc/MBA). The occupational distribution is fairly balanced among accountants (32.1%), finance officers (31.6%), and IT personnel (30.0%), while auditors represent a smaller group (6.3%). In terms of work experience, the majority (55.8%) have 2–5 years of experience, indicating a workforce that is both experienced and engaged in the operational aspects of financial and ICT systems.

Table 4.2: Impact of accounting software usage on the prevention and detection of accounting fraud in organizations

ITEM	SA	A	N	D	SD	Mean	Decision
Accounting software enhances the accuracy of financial records.	207 (54.5%)	114 (30.0%)	20 (5.3%)	20 (5.3%)	19 (5.0%)	4.24	High
The use of accounting software prevents intentional misstatement of financial reports.	209 (55.0%)	119 (31.3%)	15 (3.9%)	16 (4.2%)	21 (5.5%)	4.26	High
My organization uses accounting software to detect suspicious transactions.	20 (5.3%)	203 (53.4%)	122 (32.1%)	16 (4.2%)	19 (5.0%)	3.50	High
Accounting software reduces the risk of fraud through automation.	114 (30.0%)	201 (52.9%)	31 (8.2%)	18 (4.7%)	16 (4.2%)	4.00	High
Lack of proper use of accounting software contributes to fraud.	136 (35.8%)	131 (34.5%)	30 (7.9%)	42 (11.1%)	41 (10.8%)	3.73	High
Overall Mean	**686 (36.1%)**	**768 (40.4%)**	**218 (11.5%)**	**112 (5.9%)**	**116 (6.1%)**	**3.95**	**High**

Source: Field Survey, (2025).

Response from the table shows that 36.1% of the respondents strongly agreed that accounting software usage impacts the prevention and detection of accounting fraud in organizations, while 40.4% agreed. Additionally, 11.5% of respondents remained neutral, 5.9% disagreed, and 6.1% strongly disagreed. The overall mean score of 3.95 indicates that accounting software usage influences the prevention and detection of accounting fraud to a high extent..

Table 4.3: Role of cybersecurity measures in reducing the occurrence of accounting fraud

ITEM	SA	A	N	D	SD	Mean	Decision
My organization uses cybersecurity tools (e.g., firewalls, anti-virus) to protect financial data.	206 (54.2%)	123 (32.4%)	14 (3.7%)	18 (4.7%)	19 (5.0%)	4.26	High
Encryption and multi-factor authentication prevent unauthorized access to accounting systems.	204 (53.7%)	121 (31.8%)	24 (6.3%)	15 (3.9%)	16 (4.2%)	4.27	High
Cybersecurity weaknesses can result in accounting fraud.	237 (62.4%)	31 (8.2%)	38 (10.0%)	37 (9.7%)	37 (9.7%)	4.04	High
My organization regularly updates its cybersecurity infrastructure.	304 (80.0%)	22 (5.8%)	17 (4.5%)	20 (5.3%)	17 (4.5%)	4.52	High
Cybersecurity tools have significantly reduced accounting fraud incidents in this firm.	137 (36.1%)	136 (35.8%)	50 (13.2%)	26 (6.8%)	31 (8.2%)	3.85	High
Overall Mean	**1088 (57.3%)**	**433 (22.8%)**	**143 (7.5%)**	**116 (6.1%)**	**120 (6.3%)**	**4.19**	**High**

Source: Field Survey, (2025).

Response from the table shows that 57.3% of the respondents strongly agreed that cybersecurity measures play a role in reducing the occurrence of accounting fraud, while 22.8% agreed. Additionally, 7.5% of respondents remained neutral, 6.1% disagreed, and 6.3% strongly disagreed. The overall mean score of 4.19 indicates that cybersecurity measures contribute to reducing accounting fraud to a high extent.

Table 4.4: Effectiveness of automated internal controls in detecting and preventing fraudulent activities within accounting systems

ITEM	SA	A	N	D	SD	Mean	Decision
Automated controls are used to validate financial transactions.	207 (54.5%)	121 (31.8%)	12 (3.2%)	17 (4.5%)	23 (6.1%)	4.24	High
My organization has systems that generate real-time alerts for suspicious activities.	133 (35.0%)	148 (38.9%)	32 (8.4%)	36 (9.5%)	31 (8.2%)	3.83	High
Automation has helped reduce manual manipulation of records.	310 (81.6%)	22 (5.8%)	14 (3.7%)	20 (5.3%)	14 (3.7%)	4.56	High
Automated systems reduce the possibility of collusion in fraud.	208 (54.7%)	115 (30.3%)	13 (3.4%)	21 (5.5%)	23 (6.1%)	4.22	High
Weak internal controls increase the likelihood of fraud.	203 (53.4%)	118 (31.1%)	18 (4.7%)	18 (4.7%)	23 (6.1%)	4.21	High
Overall Mean	**1061 (55.8%)**	**524 (27.6%)**	**89 (4.7%)**	**112 (5.9%)**	**114 (6.0%)**	**4.21**	**High**

Source: Field Survey, (2025).

Response from the table shows that 55.8% of the respondents strongly agreed that automated internal controls are effective in detecting and preventing fraudulent activities

within accounting systems, while 27.6% agreed. Additionally, 4.7% of respondents remained neutral, 5.9% disagreed, and 6.0% strongly disagreed. The overall mean score of 4.21 indicates that automated internal controls are perceived to be highly effective in detecting and preventing accounting fraud.

Table 4.5: Influence of employee ICT training on reducing the likelihood of accounting fraud in organizations

ITEM	SA	A	N	D	SD	Mean	Decision
Employees in my organization are trained on ICT tools used in accounting.	302 (79.5%)	24 (6.3%)	18 (4.7%)	18 (4.7%)	18 (4.7%)	4.51	High
ICT training helps staff identify and prevent fraudulent transactions.	45 (11.8%)	229 (60.3%)	22 (5.8%)	41 (10.8%)	43 (11.3%)	3.51	High
Lack of training on ICT systems contributes to accounting fraud.	118 (31.1%)	204 (53.7%)	25 (6.6%)	17 (4.5%)	16 (4.2%)	4.03	High
My organization conducts regular ICT fraud awareness workshops.	115 (30.3%)	210 (55.3%)	16 (4.2%)	20 (5.3%)	19 (5.0%)	4.01	High
Staff with ICT skills are less likely to commit or overlook accounting fraud.	207 (54.5%)	116 (30.5%)	14 (3.7%)	27 (7.1%)	16 (4.2%)	4.24	High
Overall Mean	**787 (41.4%)**	**783 (41.2%)**	**95 (5.0%)**	**123 (6.5%)**	**112 (5.9%)**	**4.06**	**High**

Source: Field Survey, (2025).

Response from the table shows that 41.4% of the respondents strongly agreed that employee ICT training reduces the likelihood of accounting fraud in organizations, while 41.2% agreed. Additionally, 5.0% of respondents remained neutral, 6.5% disagreed, and

5.9% strongly disagreed. The overall mean score of 4.06 indicates that employee ICT training has a high influence on reducing the likelihood of accounting fraud.

4.4 Test of Hypothesis

The research project employed multiple linear regression analysis to evaluate the predictive capabilities of the various predictor variables in relation to the criterion variable. The hypotheses were tested with a p-value in the regression result. Where the p-values are greater than or equal to 0.05, the null hypotheses (H0) are not rejected, but where the p-values are less than 0.05, the null hypotheses (H0) are rejected.

Table 4.6: Regression Analysis

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.866[a]	.751	.748	1.60821

a. Predictors: (Constant), ET, AS, CS, IC

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2918.541	4	729.635	282.110	.000[b]

	Residual	969.880	375	2.586		
	Total	3888.421	379			

a. Dependent Variable: AF

b. Predictors: (Constant), ET, AS, CS, IC

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.065	.528		.124	.902
	AS	.171	.043	.182	4.003	.000
	CS	.105	.035	.129	2.956	.003
	IC	.170	.038	.213	4.445	.000
	ET	.401	.036	.444	11.249	.000

a. Dependent Variable: AF

Model Summary

The regression analysis reveals a very strong positive relationship between the independent variables Accounting Software (AS), Cybersecurity Measures (CS), Internal Control Systems (IC), and Employee ICT Training (ET) and the dependent variable, Accounting

Fraud (AF), with a correlation coefficient R = 0.866. This suggests that these predictors collectively explain a substantial portion of the variation in accounting fraud prevention and detection. The coefficient of determination, R^2 = 0.751, implies that approximately 75.1% of the variability in accounting fraud can be accounted for by the four predictors. The adjusted R^2 = 0.748, which adjusts for the number of predictors, still reflects a very high explanatory power. The standard error of the estimate (1.60821) indicates a relatively low level of prediction error, underscoring the model's robustness.

ANOVA (Model Fit)

The ANOVA table shows an F-statistic of 282.110 with a p-value of 0.000, which is well below the 0.05 threshold for statistical significance. This confirms that the overall regression model is statistically significant. Hence, we reject the null hypothesis that accounting software, cybersecurity measures, internal controls, and ICT training have no joint effect on the prevention and detection of accounting fraud. The model, therefore, is a reliable predictor of accounting fraud mitigation.

Hypothesis Interpretations

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 0.171, with a standard error of 0.043, a t-value of 4.003, and a p-value of 0.000. Since the p-value is less than 0.05, we reject H_{01}, indicating that accounting software usage significantly contributes to fraud prevention and detection. The positive coefficient suggests that effective use of accounting software plays a beneficial role in reducing fraud.

H_{02}: Cybersecurity measures do not significantly reduce the occurrence of accounting fraud in organizations

The coefficient for Cybersecurity Measures (CS) is 0.105, with a standard error of 0.035, a t-value of 2.956, and a p-value of 0.003. With the p-value below 0.05, we reject H_{02}, implying that cybersecurity measures significantly impact the reduction of accounting fraud. The positive coefficient indicates that stronger cybersecurity frameworks correlate with lower fraud risk.

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

Internal Control Systems (IC) show a coefficient of 0.170, a standard error of 0.038, a t-value of 4.445, and a p-value of 0.000. Given the statistical significance, we reject H_{03}, affirming that internal controls have a significant positive impact on detecting and preventing accounting fraud.

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

Employee ICT Training (ET) has the highest impact among the predictors, with a coefficient of 0.401, a standard error of 0.036, a t-value of 11.249, and a p-value of 0.000. The p-value confirms strong statistical significance, leading to the rejection of H_{04}. The result implies that ICT training significantly reduces accounting fraud, suggesting that well-trained employees are critical in combating fraudulent activities.

4.5 Discussion of Findings

The study investigated the roles of accounting software, cybersecurity measures, internal controls, and employee ICT training in preventing and detecting accounting fraud. All four hypotheses (H_{01} to H_{04}) were rejected due to statistically significant p-values (all < 0.05), indicating that each variable positively contributes to fraud mitigation.

Accounting Software and Fraud Detection

The findings from this study indicate a statistically significant relationship between the use of accounting software and the prevention and detection of accounting fraud, with a coefficient of 0.171 and a p-value of 0.000. This implies that the adoption and effective implementation of accounting software serve as a powerful tool in minimizing the incidence of fraudulent financial activities in organizations. The positive coefficient further supports that as organizations enhance their use of accounting software, the ability to prevent and detect fraud increases correspondingly.

These results are strongly supported by recent empirical literature. Notably, a study by Shuya Ma (2023) investigated the correlation between accounting fraud and accounting software through a comprehensive analysis of software attributes like efficiency, data accuracy, and ease of use. Ma's research emphasized that high-quality accounting software significantly reduces opportunities for fraud by improving data accuracy and making financial manipulations easier to detect. The study concluded that accounting software plays a dual role: improving performance while simultaneously serving as a safeguard against financial misconduct (Ma, 2023).

Another notable contribution comes from Hassan et al. (2023), who explored the perceptions of auditors and financial accountants on the role of both corporate governance and information technology including accounting software in fraud detection and prevention. Their findings showed that IT techniques significantly aid in reducing fraudulent activity by limiting opportunities and rationalizations for fraud. The study highlighted that accounting software, when effectively customized and integrated, can track anomalies in financial transactions and provide early fraud detection signals (Hassan et al., 2023).

Together, these studies provide solid backing for the current study's conclusion. The consistent message across the literature is that effective deployment of accounting software not only enhances operational efficiency but is also instrumental in exposing and

preventing fraudulent activities. This widespread agreement strengthens the credibility and relevance of your findings in the contemporary digital accounting landscape.

Cybersecurity Measures and Accounting Fraud

The second hypothesis, which assumed no significant impact of cybersecurity on fraud prevention, was also rejected in this study, with a coefficient of 0.105 and a p-value of 0.003. This result underscores the importance of robust cybersecurity measures in reducing the occurrence of accounting fraud within organizations. The statistically significant relationship suggests that organizations that invest in cybersecurity infrastructure such as firewalls, intrusion detection systems, and employee cybersecurity awareness are more likely to mitigate the risks associated with financial fraud.

This conclusion is corroborated by recent scholarly work, particularly the study by Abu Dabaseh and Khtatbeh (2025), which explored the influence of digital transformation, including cybersecurity maturity, on accounting fraud risk. Their research employed structural equation modeling and found a significant negative relationship between accounting fraud and well-implemented digital technologies. More importantly, cybersecurity maturity was found to strengthen this relationship, acting as a critical moderator that enhances the effectiveness of digital tools in fraud detection. The study concluded that integrating cybersecurity protocols with digital systems significantly reduces fraud vulnerability and promotes financial integrity (Abu Dabaseh & Khtatbeh, 2025).

A supporting study by Surya et al. (2024) emphasized the importance of cybersecurity awareness and education in protecting accounting information systems. Their literature review identified system vulnerabilities and human error as major causes of cyber-related fraud. They argued that mitigating such risks requires a blend of technological tools and cultural reforms within organizations. The authors concluded that cybersecurity is no longer optional; it is central to the sustainability and trustworthiness of modern accounting systems (Surya et al., 2024). Taken together, these studies reinforce the findings of the present research by demonstrating that cybersecurity plays a critical role in fraud mitigation strategies. The convergence of these findings suggests a clear pathway for organizations: investing in advanced cybersecurity infrastructure is not only a technological requirement but also a strategic decision in the fight against financial fraud.

Internal Controls and Fraud Prevention

The third hypothesis examined the effect of automated internal control systems on fraud detection and prevention. The results showed a strong statistically significant relationship, with a coefficient of 0.170 and a p-value of 0.000. This indicates that robust internal controls, particularly when automated, substantially improve an organization's ability to detect and prevent fraudulent activities. Internal controls such as segregation of duties, approval hierarchies, transaction logging, and regular audits provide multiple checkpoints that discourage and detect fraudulent behavior.

A comprehensive study by Hassan et al. (2023) lends empirical support to this result. Their research found that well-structured internal control systems, particularly those integrated with IT and audit functions, play a vital role in minimizing the potential for fraud. The auditors surveyed in their study consistently emphasized the value of strong internal oversight mechanisms in fraud detection, especially when supported by real-time monitoring tools (Hassan et al., 2023).

Additionally, Wangombe (2017) conducted a case study on the Kiambu County Government in Kenya and revealed that internal control weaknesses particularly poor communication channels, lack of reporting mechanisms, and internal audit department inefficiencies significantly contributed to fraud incidents. Her findings further highlighted the importance of risk assessment procedures and proactive fraud detection methods as key components of effective internal controls (Wangombe, 2017). These results align with this study's findings and underscore the centrality of internal control systems in a comprehensive fraud prevention strategy. The literature suggests that controls must be dynamic, consistently reviewed, and technologically integrated to remain effective in detecting increasingly sophisticated fraud tactics.

Employee ICT Training and Fraud Reduction

The final hypothesis examined the impact of employee ICT training on the occurrence of fraud in organizations. The findings showed the strongest effect among all variables, with a coefficient of 0.401 and a p-value of 0.000. This implies a robust and highly significant

relationship: organizations that prioritize training employees in ICT tools and fraud awareness are better equipped to prevent and detect fraudulent behavior.

This is strongly supported by Rekhi and Johri (2024), who conducted an extensive study in the Delhi NCR region and discovered a positive correlation between employee training programs and the effectiveness of fraud detection and prevention systems. Their results revealed that the frequency and quality of fraud awareness campaigns and ICT training significantly reduced the incidence of accounting fraud. The authors emphasized that technology adoption without corresponding employee training often leads to underutilized or misused systems, thereby weakening the fraud detection process (Rekhi & Johri, 2024).

Similarly, a study by Trehan and Shah (2024) examined the role of forensic accounting training in strengthening fraud controls within the banking sector. The findings confirmed that professionally trained employees are more adept at identifying red flags, executing preventive audits, and complying with regulatory standards. Their research supports the conclusion that education and training are not merely supplementary but foundational to an effective anti-fraud strategy (Trehan & Shah, 2024). In addition, Anomah and Agyabeng (2013) stressed the necessity of updating accounting curricula to include ICT-focused fraud detection skills. Their paper recommended that accounting professionals be trained to handle risks associated with digital accounting environments to enhance the reliability of financial statements (Anomah & Agyabeng, 2013).

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSION, AND RECCOMENDATIONS

5.1 Introduction

This chapter contains, summary of findings, the conclusion of the study, the recommendations of the study, contribution to knowledge and suggestions for further studies.

5.2 Summary of Findings

The findings from the study revealed that;

1. There is a significant relationship between the usage of accounting software and the prevention and detection of accounting fraud in organizations.
2. Cybersecurity measures, such as encryption and multi-factor authentication significantly reduce the occurrence of accounting fraud in organizations.
3. Automated internal controls significantly affect the detection and prevention of fraudulent activities within accounting systems.
4. Employee ICT training significantly reduce the occurrence of accounting fraud in organizations.

5.3 Conclusion

The study investigated the role of technological and human-centered interventions in mitigating accounting fraud within organizations, specifically examining the influence of accounting software, cybersecurity measures, internal control systems, and employee ICT training. Based on empirical evidence, all four null hypotheses were rejected, indicating that each of these components plays a significant role in either the prevention or detection of accounting fraud. The findings underscore that the integration of accounting software into organizational operations improves transparency, ensures data accuracy, and supports audit trails that help uncover inconsistencies and fraudulent transactions. Similarly, the adoption of cybersecurity measures particularly modern security protocols such as encryption, firewalls, and multi-factor authentication demonstrates a strong deterrent effect against unauthorized data manipulation and cyber-driven financial crimes.

Automated internal controls were found to be critical for reducing fraud opportunities by embedding approval processes, segregation of duties, and real-time anomaly detection into daily accounting operations. Most importantly, the study revealed that employee ICT training had the strongest impact among all variables. This highlights the importance of human capacity development in fraud prevention: well-trained employees are more vigilant, proficient in using fraud detection tools, and better equipped to follow ethical practices. In essence, the study concludes that a multifaceted approach comprising software

tools, robust cybersecurity, automated controls, and ongoing staff training is essential for building a resilient fraud-prevention framework in modern organizations.

5.4 Recommendations

Based on the conclusions of this study, the following recommendations are proposed:

1. **Organizations should invest in comprehensive accounting software** with features that allow for audit trails, transaction monitoring, and integration with other fraud detection tools. Preference should be given to systems that incorporate AI or data analytics capabilities to enhance anomaly detection.

2. **Cybersecurity infrastructure should be prioritized** as a strategic imperative. Companies must adopt modern cybersecurity protocols such as encryption, secure user authentication, periodic system vulnerability assessments, and real-time monitoring systems.

3. **Automated internal control mechanisms should be enhanced and maintained**, ensuring segregation of duties, authorization protocols, and continuous audit features are in place. These should be reviewed periodically to align with emerging fraud techniques.

4. **Regular ICT training and awareness programs for employees should be institutionalized**. These trainings must focus on both technical skills (such as how to use fraud detection tools) and soft skills (such as ethical decision-making, compliance, and reporting suspicious activity).

5.5 Suggestions for Further Studies

While this study has made valuable contributions, it also opens the door for further research in the following areas:

1. **A sector-specific analysis** could be conducted to assess whether the effects of accounting software and cybersecurity differ across industries such as banking, manufacturing, and government.
2. Future studies may explore **the mediating or moderating effects of organizational culture** or ethical leadership on the relationship between these technological tools and fraud prevention.
3. **Longitudinal studies** could be conducted to examine how the effects of ICT training and internal control evolve over time, especially in response to changes in fraud tactics and technology.
4. There is a need for **comparative studies between public and private sector organizations** to identify whether there are differences in the adoption and effectiveness of fraud prevention mechanisms.

5.0 Contribution to Knowledge

This study offers several original contributions to both academic literature and practical knowledge:

1. By analyzing four distinct but interrelated factors accounting software, cybersecurity, internal controls, and ICT training this study provides a holistic framework for understanding and combating accounting fraud in organizations.

2. The research contributes novel insight by showing that among all tested variables, ICT training has the most pronounced effect on reducing fraud, emphasizing the human dimension in fraud prevention.

3. The study translates theoretical constructs into actionable insights for practitioners, helping organizations to implement targeted interventions that reduce fraud risk.

4. By focusing on modern fraud prevention mechanisms such as automated controls and cybersecurity, the study contributes to the ongoing discourse on digital governance and organizational resilience in accounting.

REFERENCES

Adekola, O., Smith, J., & Waziri, T. (2024). Fraud in digital accounting environments: Asset misappropriation and statement manipulation. *African Journal of Accounting and Auditing*, 12(1), 45–63.

Adekola, O., Smith, J., & Waziri, T. (2024). Fraud in digital accounting environments: Asset misappropriation and statement manipulation. *African Journal of Accounting and Auditing*, 12(1), 45–63.

Adelakun, F., Peters, L., & Ojo, O. (2024). Machine learning and AI in forensic accounting: Enhancements for fraud detection. *International Journal of Digital Finance*, 5(1), 22–39.

Ahmad, A., Khan, Z., & Malik, S. (2023). Impact of digital automation on financial accuracy: A study of manual vs. ICT-enabled accounting systems. *Journal of Financial Innovation*, 8(2), 101–117.

Ali, R., & Handro, M. (2022). Technology and integrity: Perceptions of accountants and auditors on fraud prevention. *Journal of Accounting Integrity*, 6(2), 44–59.

Ali, R., Chen, Y., & Gupta, S. (2024). Forensic accounting and anomaly detection in ERP-integrated platforms. *Journal of Enterprise Systems*, 10(3), 150–168.

Baldini, L. (2023). Regulatory reforms and the detection of accounting fraud: An analysis of Italy's Law No. 69/2015. *Italian Journal of Law and Corporate Governance*, 9(1), 71–89.

Cyril, K. S., Okoro, U., & Abiola, D. (2023). The effect of information and communication technology on accounting practices and fraud prevention in Nigeria. *Nigerian Journal of Accounting and Finance*, 15(2), 110–128.

Daff, L. (2021). Employers' perspectives on ICT and software competencies for accounting graduates: Bridging the education-practice gap. *Australian Journal of Accounting Education*, 13(1), 52–67.

Dewayanto, A. (2023). Continuous auditing and data mining tools in fraud prevention. *Southeast Asian Journal of Accounting*, 9(4), 77–91.

Djuharni, T., Widiyanto, A., & Gunawan, R. (2024). Auditor and law enforcement relationships in accounting fraud detection: A systematic review. *Asian Journal of Forensic Accounting*, 8(1), 18–35.

Efuntade, T., & Efuntade, A. (2023). Digital vulnerabilities in accounting systems and control weaknesses. *Journal of Modern Accounting Research*, 11(2), 33–52.

Eghe-Ikhurhe, S., Afolayan, J., & Umeh, E. (2024). Enhancing employee awareness to mitigate cybersecurity breaches in accounting systems. *Nigerian Journal of Cybersecurity in Finance*, 2(1), 88–105.

Gomez, M. L. (2025). The impact of forensic accounting and ICT training on fraud detection self-efficacy among social security account officers. *Philippine Journal of Forensic Studies*, 7(1), 101–121.

Idrus, N., Lee, P., & Kumar, R. (2024). Cross-national analysis of forensic accounting implementation and fraud incidence. *Global Accounting Review*, 14(2), 210–233.

Judijanto, D., & Defitri, N. (2024). Interdisciplinary approaches in forensic accounting literature: A bibliometric study. *Journal of Accounting Science*, 15(1), 9–27.

Martins, J., & Francisco, M. (2021). The impact of ICT on certified accountants' practices: Perceptions from Leiria, Portugal. *European Journal of Accounting and Technology*, 8(2), 93–109.

Mobilingo, P., & Hailah, K. (2024). Cloud-based platforms and real-time financial management. *Journal of Cloud Finance*, 7(1), 1–20.

Prihanto, D., Maharani, S., & Kusumo, B. (2024). Blockchain adoption in accounting systems: Impact on audit trails. *Journal of Emerging Technology in Accounting*, 6(2), 55–70.

Rathakrishnan, R., & Baskar, V. (2024). Cybersecurity protocols and MFA in ERP security frameworks. *International Journal of Information Security & Finance*, 4(1), 101–119.

Rekhi, H., & Johri, V. (2024). Blockchain and transparency: Disruptive technologies in accounting. *Journal of Distributed Ledger Research*, 2(1), 88–105.

Subedi, R., & Neupane, S. (2024). Internal controls, monitoring mechanisms, and fraud prevention in digital accounting. *Nepalese Journal of Accounting and Finance*, 3(1), 24–41.

Tuharea, A., Morgan, L., & Patel, S. (2024). Corporate fraud typologies in ICT-driven systems: A framework for detection. *Journal of Corporate Integrity*, 11(3), 133–150.

Vutumu, C. (2024). System audits and the integrity of financial data in digital environments. *East African Journal of Accounting Technology*, 5(2), 65–82.

Wamukota, R., Onyango, D., & Obiero, F. (2022). Accounting information and communication control systems, financial performance, and fraud risk in Kenyan SACCOs. *East African Journal of Financial Systems*, 4(1), 36–54.

Werastuti, H., Nugroho, Y., & Santoso, P. (2023). Cyber threats in accounting: Encryption and firewall solutions. *Indonesian Journal of Cyberaccounting*, 1(2), 40–58.

APPENDIX I

DEPARTMENT OF ACCOUNTING

FACULTY OF ENVIRONMENTAL SCIENCES

UNIVERSITY OF BENIN

SECTION A: INTRODUCTION

Dear Respondent,

My name is Sophia Okoro, a final-year student in the Department of Accounting, Faculty of Management Sciences, University of Benin. I am conducting a research study titled:"The Impact of Information and Communication Technology (ICT) on Accounting Fraud Prevention in Private Firms in Benin City,Edo State."

This study is part of the requirements for the award of a Bachelor of Science (B.Sc.) degree in Accounting.

The objective of this questionnaire is to obtain your honest and unbiased opinions regarding the role of ICT tools such as accounting software, cybersecurity measures, automated internal controls, and employee ICT training in preventing and detecting accounting fraud in private organizations.

Please be assured that all information provided will be treated with strict confidentiality and used only for academic purposes. Your identity or that of your organization is not required,and your participation is voluntary.

Your cooperation and sincere responses will be greatly appreciated.

Thank you.

Sophia Okoro

Key to Likert Scale:

· SD=Strongly Disagree

· D=Disagrec

N=Neutral

· A=Agrcc

SA=StronglyAgree

Section A: Demographic Information

Please fill or tick the appropriate response.

1. Gender: ( )Male ( )Female

2. Age:( )18-25( )26-35 ( )36-45 ( )46 and above

3. Educational Qualification; ( )OND/NCE ( ) HND/B.Sc. ( )M.Sc./MBA ( ) Ph.D.

4. Current Position: □Accountant Auditor ( )Finance Officer ( )IT Personnel ( )Others (Specify):

5. Years of Work Experience: □Less than 2 years ( )2-5 years ( )6-10 years ( )Above 10 years

Section B: Accounting Software and Accounting Fraud

S/N	Statement	SD	D	N	A	SA
B1	Accounting software enhances the accuracy of financial records.					
B2	The use of accounting software prevents intentional misstatement of financial reports.					
B3	My organization uses accounting software to detect suspicious transactions.					
B4	Accounting software reduces the risk of fraud through automation.					

B5	Lack of proper use of accounting software contributes to fraud.					

Section C: Cybersecurity Measures and Accounting Fraud

S/N	Statement	SD	D	N	A	SA
C1	My organization uses cybersecurity tools (e.g., firewalls,anti-virus) to protect financial data.					
C2	Encryption and muIti-factor authentication prevent unauthorized access to accounting systems.					
C3	Cybersecurity weaknesses can result in accounting fraud.					
C4	My organization regularly updates its cybersecurity infrastructure.					
C5	Cybersecurity tools have significantly reduced accounting fraud incidents in this firm.					

Section D: Automated Internal Controls and Fraud Prevention

S/N	Statement	SD	D	N	A	SA
D1	Automated controls are used to validate financial transactions.					
D2	My organization has systems that generate rea-time alerts for suspicious activities.					
D3	Automation has helped reduce manual manipulation of records.					
D4	Automated systems reduce thepossibility of collusion in fraud.					

D5	Weak internal controls increase the likelihood of fraud.					

Section E: Employee **ICT Training and Fraud Risk**

S/N	Statement	SD	D	N	A	SA
E1	Employees in my organization are trained on ICT tools used in accounting.					
E2	ICT training helps staff identify and prevent fraudulent transactions.					
E3	Lack of training on ICT systems contributes to accounting fraud.					
E4	My organization conductsregular ICT fraud awareness workshops.					
E5	Staff with ICT skills are less likely to commit or overlook accounting fraud.					

APPENDIX 11: OUTPUT

```
FREQUENCIES VARIABLES=Gender Age Educational_Qualification Current_Position
Years_of_Work_Experience
  /ORDER=ANALYSIS.
```

Frequencies

Notes

Output Created		30-JUL-2025 02:49:15
Comments		
Input	Data	C:\Users\USER\Desktop\latest project 2024\data\Sophia analysis.sav
	Active Dataset	DataSet1
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	380
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on all cases with valid data.

Syntax		FREQUENCIES VARIABLES=Gender Age Educational_Qualification Current_Position Years_of_Work_Experience /ORDER=ANALYSIS.
Resources	Processor Time	00:00:00.00
	Elapsed Time	00:00:00.04

Statistics

		Gender	Age	Educational Qualification	Curent Position	Years of Work Experience
N	Valid	380	380	380	380	380
	Missing	0	0	0	0	0

Frequency Table

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	151	39.7	39.7	39.7
	Male	229	60.3	60.3	100.0
	Total	380	100.0	100.0	

Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18 - 25	18	4.7	4.7	4.7
	26 -35	211	55.5	55.5	60.3
	36 -45	123	32.4	32.4	92.6
	46 and Above	28	7.4	7.4	100.0
	Total	380	100.0	100.0	

Educational Qualification

	Frequency	Percent	Valid Percent	Cumulative Percent

Valid	HND/Bsc	224	58.9	58.9	58.9
	Msc/MBA	110	28.9	28.9	87.9
	OND	23	6.1	6.1	93.9
	PhD	23	6.1	6.1	100.0
	Total	380	100.0	100.0	

Curent Position

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Accountant	122	32.1	32.1	32.1
	Auditor	24	6.3	6.3	38.4
	Finance Officer	120	31.6	31.6	70.0
	IT Personnel	114	30.0	30.0	100.0
	Total	380	100.0	100.0	

Years of Work Experience

	Frequency	Percent	Valid Percent	Cumulative Percent

Valid	2 - 5 years	212	55.8	55.8	55.8
	6- 10 Years	124	32.6	32.6	88.4
	Above 10 years	23	6.1	6.1	94.5
	Less than 2 years	21	5.5	5.5	100.0
	Total	380	100.0	100.0	

```
FREQUENCIES VARIABLES=q1 q2 q3 q4 q5
  /STATISTICS=MEAN
  /ORDER=ANALYSIS.
```

Frequencies

Notes

Output Created		30-JUL-2025 02:50:00
Comments		
Input	Data	C:\Users\USER\Desktop\latest project 2024\data\Sophia analysis.sav
	Active Dataset	DataSet1
	Filter	<none>
	Weight	<none>
	Split File	<none>

	N of Rows in Working Data File	380
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on all cases with valid data.
Syntax		FREQUENCIES VARIABLES=q1 q2 q3 q4 q5 /STATISTICS=MEAN /ORDER=ANALYSIS.
Resources	Processor Time	00:00:00.00
	Elapsed Time	00:00:00.04

Statistics

		Accounting software enhances the accuracy of financial records.	The use of accounting software prevents intentional misstatement of financial reports.	My organization uses accounting software to detect suspicious transactions.	Accounting software reduces the risk of fraud through automation.	Lack of proper use of accounting software contributes to fraud.
N	Valid	380	380	380	380	380

	Missing	0	0	0	0	0
Mean		4.24	4.26	3.50	4.00	3.73

Frequency Table

Accounting software enhances the accuracy of financial records.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	19	5.0	5.0	5.0
	Disagree	20	5.3	5.3	10.3
	Neutral	20	5.3	5.3	15.5
	Agree	114	30.0	30.0	45.5
	Strongly Agree	207	54.5	54.5	100.0
	Total	380	100.0	100.0	

The use of accounting software prevents intentional misstatement of financial reports.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	21	5.5	5.5	5.5
	Disagree	16	4.2	4.2	9.7

	Neutral	15	3.9	3.9	13.7
	Agree	119	31.3	31.3	45.0
	Strongly Agree	209	55.0	55.0	100.0
	Total	380	100.0	100.0	

My organization uses accounting software to detect suspicious transactions.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	19	5.0	5.0	5.0
	Disagree	16	4.2	4.2	9.2
	Neutral	122	32.1	32.1	41.3
	Agree	203	53.4	53.4	94.7
	Strongly Agree	20	5.3	5.3	100.0
	Total	380	100.0	100.0	

Accounting software reduces the risk of fraud through automation.

	Frequency	Percent	Valid Percent	Cumulative Percent

Valid	Strongly Disagree	16	4.2	4.2	4.2
	Disagree	18	4.7	4.7	8.9
	Neutral	31	8.2	8.2	17.1
	Agree	201	52.9	52.9	70.0
	Strongly Agree	114	30.0	30.0	100.0
	Total	380	100.0	100.0	

Lack of proper use of accounting software contributes to fraud.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	41	10.8	10.8	10.8
	Disagree	42	11.1	11.1	21.8
	Neutral	30	7.9	7.9	29.7
	Agree	131	34.5	34.5	64.2
	Strongly Agree	136	35.8	35.8	100.0
	Total	380	100.0	100.0	

```
FREQUENCIES VARIABLES=Gender q6 q7 q8 q9 q10
  /STATISTICS=MEAN
  /ORDER=ANALYSIS.
```

Frequencies

Notes

Output Created		30-JUL-2025 02:51:10
Comments		
Input	Data	C:\Users\USER\Desktop\latest project 2024\data\Sophia analysis.sav
	Active Dataset	DataSet1
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	380
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on all cases with valid data.
Syntax		FREQUENCIES VARIABLES=Gender q6 q7 q8 q9 q10 /STATISTICS=MEAN /ORDER=ANALYSIS.
Resources	Processor Time	00:00:00.00

Elapsed Time	00:00:00.01

Statistics

		Gender	My organization uses cybersecurity tools (e.g., firewalls, anti-virus) to protect financial data.	Encryption and multi-factor authentication prevent unauthorized access to accounting systems.	Cybersecurity weaknesses can result in accounting fraud.	My organization regularly updates its cybersecurity infrastructure.
N	Valid	380	380	380	380	380
	Missing	0	0	0	0	0
Mean			4.26	4.27	4.04	4.52

Statistics

		Cybersecurity tools have significantly reduced accounting fraud incidents in this firm.
N	Valid	380
	Missing	0
Mean		3.85

Frequency Table

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	151	39.7	39.7	39.7
	Male	229	60.3	60.3	100.0
	Total	380	100.0	100.0	

My organization uses cybersecurity tools (e.g., firewalls, anti-virus) to protect financial data.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	19	5.0	5.0	5.0
	Disagree	18	4.7	4.7	9.7
	Neutral	14	3.7	3.7	13.4
	Agree	123	32.4	32.4	45.8
	Strongly Agree	206	54.2	54.2	100.0
	Total	380	100.0	100.0	

Encryption and multi-factor authentication prevent unauthorized access to accounting systems.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	16	4.2	4.2	4.2
	Disagree	15	3.9	3.9	8.2
	Neutral	24	6.3	6.3	14.5
	Agree	121	31.8	31.8	46.3
	Strongly Agree	204	53.7	53.7	100.0
	Total	380	100.0	100.0	

Cybersecurity weaknesses can result in accounting fraud.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	37	9.7	9.7	9.7
	Disagree	37	9.7	9.7	19.5
	Neutral	38	10.0	10.0	29.5
	Agree	31	8.2	8.2	37.6
	Strongly Agree	237	62.4	62.4	100.0
	Total	380	100.0	100.0	

My organization regularly updates its cybersecurity infrastructure.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	17	4.5	4.5	4.5
	Disagree	20	5.3	5.3	9.7
	Neutral	17	4.5	4.5	14.2
	Agree	22	5.8	5.8	20.0
	Strongly Agree	304	80.0	80.0	100.0
	Total	380	100.0	100.0	

Cybersecurity tools have significantly reduced accounting fraud incidents in this firm.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	31	8.2	8.2	8.2
	Disagree	26	6.8	6.8	15.0
	Neutral	50	13.2	13.2	28.2
	Agree	136	35.8	35.8	63.9
	Strongly Agree	137	36.1	36.1	100.0
	Total	380	100.0	100.0	

```
FREQUENCIES VARIABLES=q11 q12 q13 q14 q15
  /STATISTICS=MEAN
  /ORDER=ANALYSIS.
```

Frequencies

Notes

Output Created		30-JUL-2025 02:52:22
Comments		
Input	Data	C:\Users\USER\Desktop\latest project 2024\data\Sophia analysis.sav
	Active Dataset	DataSet1
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	380
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on all cases with valid data.

Syntax		FREQUENCIES VARIABLES=q11 q12 q13 q14 q15 /STATISTICS=MEAN /ORDER=ANALYSIS.
Resources	Processor Time	00:00:00.00
	Elapsed Time	00:00:00.01

Statistics

		Automated controls are used to validate financial transactions.	My organization has systems that generate real-time alerts for suspicious activities.	Automation has helped reduce manual manipulation of records.	Automated systems reduce the possibility of collusion in fraud.	Weak internal controls increase the likelihood of fraud.
N	Valid	380	380	380	380	380
	Missing	0	0	0	0	0
Mean		4.24	3.83	4.56	4.22	4.21

Frequency Table

Automated controls are used to validate financial transactions.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	23	6.1	6.1	6.1
	Disagree	17	4.5	4.5	10.5
	Neutral	12	3.2	3.2	13.7
	Agree	121	31.8	31.8	45.5
	Strongly Agree	207	54.5	54.5	100.0
	Total	380	100.0	100.0	

My organization has systems that generate real-time alerts for suspicious activities.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	31	8.2	8.2	8.2
	Disagree	36	9.5	9.5	17.6
	Neutral	32	8.4	8.4	26.1
	Agree	148	38.9	38.9	65.0
	Strongly Agree	133	35.0	35.0	100.0

	Total	380	100.0	100.0	

Automation has helped reduce manual manipulation of records.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	14	3.7	3.7	3.7
	Disagree	20	5.3	5.3	8.9
	Neutral	14	3.7	3.7	12.6
	Agree	22	5.8	5.8	18.4
	Strongly Agree	310	81.6	81.6	100.0
	Total	380	100.0	100.0	

Automated systems reduce the possibility of collusion in fraud.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	23	6.1	6.1	6.1
	Disagree	21	5.5	5.5	11.6
	Neutral	13	3.4	3.4	15.0

	Agree	115	30.3	30.3	45.3
	Strongly Agree	208	54.7	54.7	100.0
	Total	380	100.0	100.0	

Weak internal controls increase the likelihood of fraud.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	23	6.1	6.1	6.1
	Disagree	18	4.7	4.7	10.8
	Neutral	18	4.7	4.7	15.5
	Agree	118	31.1	31.1	46.6
	Strongly Agree	203	53.4	53.4	100.0
	Total	380	100.0	100.0	

```
FREQUENCIES VARIABLES=q16 q17 q18 q19 q20
  /STATISTICS=MEAN
  /ORDER=ANALYSIS.
```

Frequencies

Notes

Output Created		30-JUL-2025 02:53:39
Comments		
Input	Data	C:\Users\USER\Desktop\latest project 2024\data\Sophia analysis.sav
	Active Dataset	DataSet1
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	380
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on all cases with valid data.

Syntax		FREQUENCIES VARIABLES=q16 q17 q18 q19 q20 /STATISTICS=MEAN /ORDER=ANALYSIS.
Resources	Processor Time	00:00:00.02
	Elapsed Time	00:00:00.01

Statistics

		Employees in my organization are trained on ICT tools used in accounting.	ICT training helps staff identify and prevent fraudulent transactions.	Lack of training on ICT systems contributes to accounting fraud.	My organization conducts regular ICT fraud awareness workshops.	Staff with ICT skills are less likely to commit or overlook accounting fraud.
N	Valid	380	380	380	380	380
	Missing	0	0	0	0	0
Mean		4.51	3.51	4.03	4.01	4.24

Frequency Table

Employees in my organization are trained on ICT tools used in accounting.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	18	4.7	4.7	4.7
	Disagree	18	4.7	4.7	9.5
	Neutral	18	4.7	4.7	14.2
	Agree	24	6.3	6.3	20.5
	Strongly Agree	302	79.5	79.5	100.0
	Total	380	100.0	100.0	

ICT training helps staff identify and prevent fraudulent transactions.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	43	11.3	11.3	11.3
	Disagree	41	10.8	10.8	22.1
	Neutral	22	5.8	5.8	27.9
	Agree	229	60.3	60.3	88.2
	Strongly Agree	45	11.8	11.8	100.0

	Total	380	100.0	100.0	

Lack of training on ICT systems contributes to accounting fraud.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	16	4.2	4.2	4.2
	Disagree	17	4.5	4.5	8.7
	Neutral	25	6.6	6.6	15.3
	Agree	204	53.7	53.7	68.9
	Strongly Agree	118	31.1	31.1	100.0
	Total	380	100.0	100.0	

My organization conducts regular ICT fraud awareness workshops.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	19	5.0	5.0	5.0
	Disagree	20	5.3	5.3	10.3
	Neutral	16	4.2	4.2	14.5

	Agree	210	55.3	55.3	69.7
	Strongly Agree	115	30.3	30.3	100.0
	Total	380	100.0	100.0	

Staff with ICT skills are less likely to commit or overlook accounting fraud.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	16	4.2	4.2	4.2
	Disagree	27	7.1	7.1	11.3
	Neutral	14	3.7	3.7	15.0
	Agree	116	30.5	30.5	45.5
	Strongly Agree	207	54.5	54.5	100.0
	Total	380	100.0	100.0	

```
REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
```

/DEPENDENT AF

/METHOD=ENTER AS CS IC ET.

Regression

Notes

Output Created		30-JUL-2025 02:54:26
Comments		
Input	Data	C:\Users\USER\Desktop\latest project 2024\data\Sophia analysis.sav
	Active Dataset	DataSet1
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	380
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on cases with no missing values for any variable used.

Syntax		REGRESSION /MISSING LISTWISE /STATISTICS COEFF OUTS R ANOVA /CRITERIA=PIN(.05) POUT(.10) /NOORIGIN /DEPENDENT AF /METHOD=ENTER AS CS IC ET.
Resources	Processor Time	00:00:00.02
	Elapsed Time	00:00:00.02
	Memory Required	5360 bytes
	Additional Memory Required for Residual Plots	0 bytes

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	ET, AS, CS, IC[b]	.	Enter

a. Dependent Variable: AF

b. All requested variables entered.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.866[a]	.751	.748	1.60821

a. Predictors: (Constant), ET, AS, CS, IC

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2918.541	4	729.635	282.110	.000[b]
	Residual	969.880	375	2.586		
	Total	3888.421	379			

a. Dependent Variable: AF

b. Predictors: (Constant), ET, AS, CS, IC

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	.065	.528		.124	.902
	AS	.171	.043	.182	4.003	.000
	CS	.105	.035	.129	2.956	.003
	IC	.170	.038	.213	4.445	.000
	ET	.401	.036	.444	11.249	.000

a. Dependent Variable: AF

20% Overall Similarity

Top sources found in the following databases:

- 15% Internet database
- 7% Publications database
- Crossref database
- 16% Submitted Works database

TOP SOURCES

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	University of Worcester on 2025-09-12 Submitted works	1%
2	dspace.univ-msila.dz Internet	<1%
3	etd.aau.edu.et Internet	<1%
4	coursehero.com Internet	<1%
5	ujm.com.ng Internet	<1%
6	benin on 2025-08-29 Submitted works	<1%
7	Kisii University on 2019-08-27 Submitted works	<1%
8	ir.uew.edu.gh:8080 Internet	<1%
9	projectreserve.com Internet	<1%

10	University of Glamorgan on 2024-09-22 Submitted works	<1%
11	CVC Nigeria Consortium on 2015-05-05 Submitted works	<1%
12	blog.osum.com Internet	<1%
13	Syed Waleed Ul Hassan, Samra Kiran, Samina Gul, Ibrahim N. Khatatbe... Crossref	<1%
14	researchgate.net Internet	<1%
15	University of Teesside on 2025-05-08 Submitted works	<1%
16	mis.itmuniversity.ac.in Internet	<1%
17	Hanzehogeschool Groningen on 2025-08-27 Submitted works	<1%
18	mdpi.com Internet	<1%
19	Abubakar Abubakar. "Digital Transformation Initiatives for Effective Di... Crossref	<1%
20	doaj.org Internet	<1%
21	ir-library.ku.ac.ke Internet	<1%

22	Ajou University Graduate School on 2024-06-12 Submitted works	<1%
23	Meiryani Meiryani, Vidhiya Andini, Mochammad Fahlevi, Winwin Yadiat... Crossref	<1%
24	afropolitanjournals.com Internet	<1%
25	National Open University of Nigeria on 2021-07-30 Submitted works	<1%
26	repository.lcu.edu.ng Internet	<1%
27	Federal University of Technology on 2025-10-13 Submitted works	<1%
28	University of Bradford on 2024-03-26 Submitted works	<1%
29	rgu-repository.worktribe.com Internet	<1%
30	Higher Education Commission Pakistan on 2024-10-28 Submitted works	<1%
31	Aloysius Vutumu, Sebil Olalekan Oshota, Ademola S. Akinteye. "Forens... Crossref	<1%
32	Liverpool John Moores University on 2024-04-14 Submitted works	<1%
33	ir.knust.edu.gh Internet	<1%

34	Kristy Soh on 2025-10-05 Submitted works	<1%
35	University of Sri Jayewardenepura Nugegoda Sri Lanka on 2025-08-03 Submitted works	<1%
36	Ishik University on 2024-05-07 Submitted works	<1%
37	University of Sunderland on 2012-09-12 Submitted works	<1%
38	BBS on 2025-09-17 Submitted works	<1%
39	ijnrd.org Internet	<1%
40	meral.edu.mm Internet	<1%
41	researchspace.ukzn.ac.za Internet	<1%
42	phd-dissertations.unizik.edu.ng Internet	<1%
43	ecohumanism.co.uk Internet	<1%
44	lbrucepublications.com Internet	<1%
45	Dublin Business School on 2025-08-28 Submitted works	<1%

46	Institute of Graduate Studies, UiTM on 2017-05-02 Submitted works	<1%
47	KDU College Sdn Bhd on 2009-04-09 Submitted works	<1%
48	Li Wei, Chalermkiat Wongvanichtawee, Chia-Hsien Tang. "The role of tr... Crossref	<1%
49	National School of Business Management NSBM, Sri Lanka on 2025-0... Submitted works	<1%
50	Universiti Teknologi MARA on 2014-06-30 Submitted works	<1%
51	pdfs.semanticscholar.org Internet	<1%
52	grin.com Internet	<1%
53	1library.net Internet	<1%
54	eprints.utar.edu.my Internet	<1%
55	techsciresearch.com Internet	<1%
56	Federal Polytechnic, Ilaro on 2025-09-10 Submitted works	<1%
57	Institute of Graduate Studies, UiTM on 2015-01-09 Submitted works	<1%

58	Maria Assunta Baldini. "Risks of false accounting: Some reflections on ... Crossref	<1%
59	ijsea.com Internet	<1%
60	University of Northampton on 2023-09-20 Submitted works	<1%
61	Higher Education Commission Pakistan on 2010-05-28 Submitted works	<1%
62	Rivers State University of Science & Technology on 2019-03-17 Submitted works	<1%
63	Temple University on 2024-03-17 Submitted works	<1%
64	acespedunn.edu.ng Internet	<1%
65	ijsre.com Internet	<1%
66	Universiti Selangor on 2018-01-09 Submitted works	<1%
67	University Tun Hussein Onn Malaysia on 2020-12-21 Submitted works	<1%
68	hal.science Internet	<1%
69	grossarchive.com Internet	<1%

70	Hewa Majeed Zangana, Rindah Febriana Suryawati, Firas Mahmood M... Crossref	<1%
71	Higher Education Commission Pakistan on 2010-01-15 Submitted works	<1%
72	Liverpool John Moores University on 2023-11-30 Submitted works	<1%
73	Sheffield Hallam University on 2025-09-04 Submitted works	<1%
74	Swiss School of Business and Management - SSBM on 2024-05-31 Submitted works	<1%
75	eprints.gouni.edu.ng Internet	<1%
76	Dr. Jason Edwards. "Critical Security Controls for Effective Cyber Defe... Crossref	<1%
77	Islamic Azad University on 2015-11-09 Submitted works	<1%
78	University of Glamorgan on 2024-08-01 Submitted works	<1%
79	eprints.kingston.ac.uk Internet	<1%
80	etd.cput.ac.za Internet	<1%
81	keffi.nsuk.edu.ng Internet	<1%

82	mail.jrtdd.com Internet	<1%
83	openscholar.dut.ac.za Internet	<1%
84	sociologiecraiova.ro Internet	<1%
85	oer.unn.edu.ng Internet	<1%
86	Brunel University on 2025-03-20 Submitted works	<1%
87	Dinah Koteikor Baidoo, Williams E. Nwagwu. "User and service provider... Crossref	<1%
88	Frisco Harmadi, Ika Maryani, Sukirman Sukirman, Elsa Carmen N Mont... Crossref	<1%
89	Global Banking Training on 2025-02-08 Submitted works	<1%
90	National School of Business Management NSBM, Sri Lanka on 2025-0... Submitted works	<1%
91	rikinstitute.com Internet	<1%
92	dataideology.com Internet	<1%
93	globalscientificjournal.com Internet	<1%

94	greaterbirminghamchambers.com Internet	<1%
95	Banking Academy on 2025-03-09 Submitted works	<1%
96	Mansoura University on 2025-09-19 Submitted works	<1%
97	Newman College on 2020-11-23 Submitted works	<1%
98	University of Northumbria at Newcastle on 2022-09-24 Submitted works	<1%
99	docslib.org Internet	<1%
100	flex.flinders.edu.au Internet	<1%
101	repository.smuc.edu.et Internet	<1%
102	Asia Pacific University College of Technology and Innovation (UCTI) on... Submitted works	<1%
103	National School of Business Management NSBM, Sri Lanka on 2025-1... Submitted works	<1%
104	core.ac.uk Internet	<1%
105	eprints.kwikkiangie.ac.id Internet	<1%

106	etd.uum.edu.my Internet	<1%
107	ir.lib.uwo.ca Internet	<1%
108	ijrdo.org Internet	<1%
109	theseus.fi Internet	<1%
110	Federal University of Technology on 2017-08-08 Submitted works	<1%
111	Gunawan Widjaja. "Managing Legal and Corporate Compliance to Indu... Publication	<1%
112	Strathmore University (Main Account) on 2025-07-07 Submitted works	<1%
113	University of Northampton on 2025-09-01 Submitted works	<1%
114	ir.kiu.ac.ug Internet	<1%
115	cscanada.net Internet	<1%
116	Anqi Rong, Nina Hansopaheluwakan-Edward, Dian Li. "Visualizing invis... Crossref	<1%
117	Asia Pacific University College of Technology and Innovation (UCTI) on... Submitted works	<1%

118	University of Bucharest on 2025-10-22 Submitted works	<1%
119	University of Hull on 2024-09-04 Submitted works	<1%
120	ch.vi.wikimiki.org Internet	<1%
121	psychosocial.com Internet	<1%
122	Alex Khang. "AI-Powered Cybersecurity for Banking and Finance - How ... Publication	<1%
123	Asia Pacific University College of Technology and Innovation (UCTI) on... Submitted works	<1%
124	De Montfort University on 2024-04-09 Submitted works	<1%
125	Segi University College on 2013-05-10 Submitted works	<1%
126	University of Northumbria at Newcastle on 2024-05-23 Submitted works	<1%
127	rsisinternational.org Internet	<1%
128	statetimes.in Internet	<1%
129	Ateneo de Davao University on 2023-03-03 Submitted works	<1%

130	Capella University on 2024-04-16 Submitted works	<1%
131	Hafinaz, R Hariharan, R. Senthil Kumar. "Recent Research in Managem... Publication	<1%
132	Mansoura University on 2025-09-13 Submitted works	<1%
133	Mount Kenya University on 2025-10-18 Submitted works	<1%
134	Queensland University of Technology on 2024-05-12 Submitted works	<1%
135	SCHOOL OF BUSINESS (SOB) on 2025-10-11 Submitted works	<1%
136	University of Nigeria on 2024-04-25 Submitted works	<1%
137	University of Ulster on 2024-06-05 Submitted works	<1%
138	Weber State University on 2013-10-09 Submitted works	<1%
139	centaur.reading.ac.uk Internet	<1%
140	eprajournals.com Internet	<1%
141	fastercapital.com Internet	<1%

142	ir.jkuat.ac.ke Internet	<1%
143	ojbe.steconomiceuoradea.ro Internet	<1%
144	iaset.us Internet	<1%
145	Athlone Institute of Technology on 2024-08-12 Submitted works	<1%
146	Bharati Vidyapeeth Deemed University College Of Engineering on 2017... Submitted works	<1%
147	HELP UNIVERSITY on 2015-12-02 Submitted works	<1%
148	Leeds Beckett University on 2025-09-21 Submitted works	<1%
149	Monash University on 2021-09-15 Submitted works	<1%
150	The University of the West of Scotland on 2024-07-11 Submitted works	<1%
151	Trident University International on 2025-04-14 Submitted works	<1%
152	Zambia Centre for Accountancy Studies on 2025-09-21 Submitted works	<1%
153	eprint.innovativepublication.org Internet	<1%

154	erepository.uonbi.ac.ke Internet	<1%
155	mafiadoc.com Internet	<1%
156	una.edu Internet	<1%
157	williamsonwines.com Internet	<1%
158	chicagopolice.org Internet	<1%
159	360research.blogspot.com Internet	<1%
160	Asia Pacific Instutute of Information Technology on 2023-02-27 Submitted works	<1%
161	Asia Pacific University College of Technology and Innovation (UCTI) on... Submitted works	<1%
162	Flinders University on 2023-11-05 Submitted works	<1%
163	Gulf University for Science & Technology on 2024-12-26 Submitted works	<1%
164	Heriot-Watt University on 2024-02-26 Submitted works	<1%
165	Higher Education Commission Pakistan on 2025-03-04 Submitted works	<1%

166	ICTS on 2025-10-21 Submitted works	<1%
167	Ignatius Ajuru University of Education on 2022-05-09 Submitted works	<1%
168	Leeds Beckett University on 2025-09-22 Submitted works	<1%
169	Open University Malaysia on 2009-02-16 Submitted works	<1%
170	Pawan Kumar, Mukul Bhatnagar, Bhupinder Pal Singh Chahal, Sanjay T... Crossref	<1%
171	Saito University College on 2025-09-29 Submitted works	<1%
172	Singapore Institute of Technology on 2024-08-11 Submitted works	<1%
173	Southern New Hampshire University - Continuing Education on 2025-0... Submitted works	<1%
174	Universiti Teknologi MARA on 2025-10-22 Submitted works	<1%
175	University College for the Creative Arts at Canterbury, Epsom, Farnham... Submitted works	<1%
176	University of Essex on 2024-09-18 Submitted works	<1%
177	University of Glasgow on 2021-04-18 Submitted works	<1%

178	University of Northumbria at Newcastle on 2025-01-13 Submitted works	<1%
179	University of Southampton on 2023-09-14 Submitted works	<1%
180	University of Strathclyde on 2009-04-01 Submitted works	<1%
181	University of Teesside on 2025-08-18 Submitted works	<1%
182	erepository.mkuit.ac.rw Internet	<1%
183	irbackend.mubs.ac.ug Internet	<1%
184	journal.fudutsinma.edu.ng Internet	<1%
185	journals.unizik.edu.ng Internet	<1%
186	journalsglobal.com Internet	<1%
187	mail.grossarchive.com Internet	<1%
188	mmcalumni.ca Internet	<1%
189	mpra.ub.uni-muenchen.de Internet	<1%

190	repository.out.ac.tz Internet	<1%
191	uwcscholar.uwc.ac.za:8443 Internet	<1%
192	wiredspace.wits.ac.za Internet	<1%
193	citcglobal.com Internet	<1%
194	udsspace.uds.edu.gh Internet	<1%
195	yumpu.com Internet	<1%
196	www02.iproject.com.ng Internet	<1%