INTEGRATION OF INFORMATION COMMUNICATION TECHNOLOGY AND PERFORMANCE OF FRAUD INVESTIGATORS AT DIRECTORATE OF CRIMINAL INVESTIGATIONS, KENYA

Mutoka Dennis.
Student, Master of Arts Public Policy and Administration, Kenyatta University, Kenya.
Prof. Minja David.
Department of Public Policy and Administration, School of Law, Arts and Social Sciences, Kenyatta University, Kenya.

International Academic Journal of Arts and Humanities (IAJAH) | ISSN 2520-4688

Received: 7th September 2024

Published: 15th September 2024

Full Length Research

Available Online at: https://iajournals.org/articles/iajah_v1_i4_314_338.pdf

Citation: Mutoka, D., Minja, D. (2024). Integration of information communication technology and performance of fraud investigators at Directorate of Criminal Investigations, Kenya. *International Academic Journal of Arts and Humanities, 1(4), 314-338.*

ABSTRACT

Fraud entails the deliberate misappropriation the organizational resources for personal benefit using one's occupation. The action is deliberate is characterized by concealment, violation of trust, and deception with the aim of embezzling the resources of an organization for personal gains. Fraud investigation entails the process of evidence collection and examination with regard to the alleged or suspected fraud to establish whether fraud, theft, or deception occurred. The study sought to establish the effect of ICT in collecting evidence on fraud investigators performance, and the effect of ICT in examining evidence on the performance of fraud investigators within the DCI, Kenya. The theories guiding the study included the theory of reasoned action, diffusion of innovation theory, and technology acceptance model. The investigation adopted a descriptive research design with a target population involving the Directorate of Criminal Investigations officers working at the Directorate of Criminal Investigations headquarters in Kiambu Road Nairobi totaling 565 respondents. Probability sampling was used in selecting a sample while stratified sampling was used to select respondents from various units. Primary data was adopted and was collected using structured questionnaires. SPSS version 26 was utilized in data analysis, which included both descriptive and inferential statistics. Descriptive results involved frequency and percentages. Inferential analysis entailed correlation and regression analysis. The study found that the integration of ICT in the collection of fraud evidence has a significant and positive effect on the performance of fraud investigators with a beta level of 0.47 and a significance level of 0.000<0.05. Furthermore, the integration of ICT in the examination of fraud evidence has a significant and positive effect on the performance of fraud investigators with a beta level of 0.418 and a significance level of 0.000<0.05. The study thus concluded that the integration of ICT in fraud evidence collection, examination, processing, and preservation has a positive and significant effect on the performance of fraud investigators. The study recommended that the DCI ought to fully adopt ICT in its process of collecting fraud in various departments. As technology advances, so are fraudsters. The adoption of ICT should be included in the process of fraud evidence collection by making it easy for witnesses and suspects to record statements. The DCI should also utilize ICT in the examination of fraud evidence collected.

Key words: ICT, Fraud Evidence, Fraud Examination and Performance of Fraud Investigators

INTRODUCTION

Information communication technology has affected every aspect of life and ICT skills have formed a common place in most social, economic, and government interactions. ICT has enabled high-level intelligence in operation, responsiveness, visibility, and coordination (Wicaksana, Kurnia, Ho, & Samson, 2021). Thus, to fraud investigators, information communication technology has enhanced their coordination, responsiveness, and intelligence in their fraud investigations. Owing to the significance of technology, the fraud investigators ought to utilize technology as they carry out their roles. ICT entails the utilization of scientific techniques and tools in the development, documentation, and communication of information when required more so as it concerns the provision of the essential services and providing solutions to problems in various areas of human interactions (Akinbowale, 2018).

Fraud entails the deliberate misappropriation of organizational resources for personal benefit using one's occupation (Lord & Levi, 2023. The action is deliberate is characterized by concealment, trust violation, and deception with the aim of siphoning the resources of an organization for individual gains (Akinbowale, Klingelhöfer, & Zerihun, 2023); Baz, Samsudin & Che Ahmad, 2017). Fraud and the intention to commit fraud is a dynamic phenomenon that is hard to be eliminated. It entails the methods that are applied by one individual with the sole aim of taking advantage of another individual through false representations (Akinbowale, Mashigo & Zerihun, 2023). Corporate fraud could also be in the form of conversion of organizational assets to personal use, theft, falsification of records, or forgery (Rashid, Al-Mamun, Roudaki & Yasser, 2022).

Fraud investigation entails the process of evidence collection and examination with regard to the alleged or suspected fraud to establish whether fraud, theft, or deception occurred (Felix, 2022). The effect of fraud on organizations could be damaging and may lead to reputational loss, dissatisfaction of customers, and operational inefficiencies among others. Thus, the incidences of fraud must be minimized and tackled for the organization to achieve profitability, goodwill, and operational excellence (Levi, 2017). Fraud detection and investigation in organizations is over time becoming complex and dynamic. This is coupled with the fact that in this digital error, the process of detecting and investigating fraud is marked with concealment, deception, and conspiracy, which makes the whole process complex in unraveling the root cause of fraud as well as the perpetrators (Felix, 2022).

ICT can be applied by law enforcement officials to identify suspected criminals through digital forensics. ICT reduces errors and facilitates the aggregation of information and hence enhances the capability of processing information. Providing proof in cyberspace is different from providing proof for conventional crimes (Mugisha, 2019). Another technique that can be applied by fraud investigators in detecting fraud is machine learning, which is a subset of artificial intelligence, and its algorithms can learn from data and improve over time without being explicitly programmed, thus providing dynamic and adaptive fraud detection solutions (Stojanović et al., 2021).

The tools utilized in data analytics contribute significantly to the success in the mitigation of fraud by forensic accounting officers (Akinbowale, Klingelhöfer & Zerihun, 2020). In emerging economies, forensic accounting faces challenges specifically due to the quality of data analytical tools deployed in fraud investigation and further due to deficiencies in expertise and skills. Thus, the quality and the pace at which forensic accounting is done in these countries is slow (Akhidime & Uagbale-Ekatah, 2014). The quality of expertise and skills of forensic investigators largely determines the type of data analytical tools to be deployed and by extension the quality of forensic investigation as well as its outcomes. Because of technological advancements, the complexity of forensic investigation in organizations is also increasingly becoming complex and dynamic. The changes in accounting policies, procedures, and principles as well as the dynamic nature of the fraudulent schemes further make the process of forensic investigation complex (Mandal, 2023). This is coupled with the fact that in this digital error, the process of detecting and investigating fraud is marked with concealment, deception, and conspiracy, which makes the whole process complex in unraveling the root cause of fraud as well as the perpetrators (Gottschalk, 2022). Thus, a mix of the experience of forensic accountants, skills and knowledge plays a critical role in fraud detection.

Several factors make that it hard for the police to investigate fraud including collecting evidence, tampering of evidence by perpetrators, and problems in storing evidence for judicial proceedings, (Maluleke, 2023; Van Dasselaar et al., 2022). According to Haq, Barthos and Fakrulloh, (2023) ICT plays an essential role in remaking violations, defending proof and providing a guarantee that the accumulated proof would stand the litigation test. This is because the law enforcement officials act in response to the actions of criminals of destroying evidence and protecting themselves (Gottschalk, 2023). ICT has enabled high-level intelligence in operation, responsiveness, visibility, and coordination and its application in detecting fraud is timely (Fysarakis et al., 2023). In Kenya, DCI is mandated to conduct criminal intelligence on economic crimes including money laundering and fraud as provided for by the National Police Act 2011.

The US has witnessed the evolution of forensic accounting necessary to curb the complexities of modern financial environments and the challenges posed by sophisticated digital financial fraud schemes. The advent of technology has been a double-edged sword in which on one hand it has led to the efficiency and effectiveness of various business activities while on the other hand has led to the advent of cybercrimes including credit card fraud, online banking fraud and identity theft (Akinbowale, Klingelhöfer & Zerihun, 2020). Thus, the evolution of forensic accounting has been marked by the integration of advanced technologies and methodologies in forensic accounting practices, reshaping the way financial fraud is investigated and detected. ICT-based forensic accounting tools have significantly increased the accuracy and speed of fraud detection during forensic investigations. They have also enhanced the performance of the investigators by providing timely and accurate evidence for financial reporting and litigation support as well as performing thorough investigations in a shorter time (Daraojimba et al., 2023).

China has in recent years reported increasing cases of financial fraud due to the dynamic nature of fraud within the listed companies. As a result of traditional fraud detection methods coupled with limited human resources, the China Securities Regulatory Commission takes so long to prove administrative penalty notices to the listed companies for suspected financial fraud commission (Chen & Wu, 2022). To improve auditing efficiency therefore, Machine learning was introduced in China as a tool for effective fraud detection since it has the capacity of efficiently detecting hidden rules in massive data. Machine learning categorizes financial fraud as a classification task (Xiuguo & Shengyong, 2022).

The victims of cybercrime in the UK are considered unlikely to immediately report crimes because of the perception that the UK police are not well equipped to deal with the crimes. Compared to victims of traditional crime, victims of cybercrime may not report the crimes to law enforcement partly because of the perception that police lack cyber knowledge and that the police may not be well equipped to deal with the crime (Button et al., 2022). Statistics indicate that 15.3% of the estimated total victims of cyber fraud report their cases to law enforcement compared to 54.5% of the victims of theft offenses. Some of the challenges faced by the police in investigating cybercrimes is practical and additional legal challenges. As legislations are continuously revised to conform to the dynamic nature of the crime, the legislations surround issues to do with technology, suspects and the geographical location of victims (Parpworth et al., 2022).

Recently, there have been significant changes in the banking industry in Nigeria. This was occasioned by cases of cyber security that had been reported in the recent years including dollar theft, extortion by armed and unarmed persons, ATM card cloning, debiting communications and authorization/non-receipt (Oni, Berepubo, Oni and Joshua (2019). There have been significant technological advancements, which have resulted in convenience, efficiency and improved accessibility of financial services. On the same note, cybercriminals have also benefited from the advancement in technology to defraud customers. This has forced financial institutions to improve on their systems especially electronic banking systems (Fatoki, 2023). The banking industry in South Africa is comparable to the financial institutions in developed countries in terms of its development and sophistication. However, fraud risk has been inherent despite its sophistication. There, the industry has put in place measures to curb these fraudulent activities. Thus, the banks have adopted information communication technology as well as enhanced internal measures. Forensic accounting entails the process of investigating suspected cyber fraud. However, digital forensics entails the process of investigating, acquiring, and discovering information that is connected to digital devices that enable digital storage of information. Adhering strictly to the provided guidelines during the process of collecting fraud evidence and the analysis of the evidence before and during investigations is a recipe for successful litigation (Akinbowale, Klingelhöfer & Zerihun, 2023).

Kenya has witnessed high-profile cases including the Afya House scandal, NYS, and Eurobond that resulted in losses of huge amounts of money. According to a global economic survey by PWC in 2018, globally Kenya has an economic crime reporting rate of 77% while it ranks second in Africa with a reporting rate of 75%. This explains the loopholes existing in the traditional audit approaches. Auditors have also failed to take responsibility for such losses. (Okemwa & Nasieku, 2023). Thus, appropriate internal control measures of curbing fraud are necessary to reduce the losses occasioned by fraud. The measures entail the procedures, methods, and plans of an organization to safeguard its assets and meet its objectives, mismanagement, fraud, and detecting and preventing errors. In the context of fraud detection, internal control operates by evaluating and monitoring activities for signs of irregularities and monitoring processes and transactions (Musyoki, 2023).

The government of Kenya has adopted technology in the delivery of government services including e-health, e-cities, e-passport, e-citizen, one-border stops, e-customs, and e-tax among others. In the 21st Century, there has been an exponential surge in the number of businesses that have been affected by data breaches and so have the opportunities, challenges, and risks associated with it. Among the noted data breaches included system interference and unauthorized access to a network which poses a threat to e-government services and can lead to possible system disruptions, destructions, alterations, data loss, phishing, system capture, and data loss (Ohndyl, Kimuyu & Sidha 2023).

Statement of the Problem

Fraud entails the deliberate organizational resource misappropriation for personal benefit using one's occupation. The action is deliberate is characterized by concealment, violation of trust, and deception with the aim of siphoning the resources of an organization for personal gains. Fraud investigation entails the process of evidence collection and examination with regard to the alleged or suspected fraud to establish whether fraud, theft, or deception occurred. Several factors that make it hard for the police to investigate fraud include collecting, evidence, tampering of evidence by perpetrators, and problems in storing evidence for judicial proceedings, (Maluleke, 2023; Van Dasselaar et al., 2022). In addition, fraud perpetrators are knowledgeable in destroying evidence. As such, the application of ICT in solving such security problems from fraud is essential.

Research studies have been carried out around the integration of ICT in fraud investigation and mitigation. Akinbowale et al (2020) in a study of an innovative approach in dealing with economic crimes with the use of forensic techniques of accounting the results indicated that the advent of technology has led to the efficiency and effectiveness of various business activities but also to the advent of cybercrimes including identity theft, online banking fraud, and credit card fraud. The evolution of forensic accounting has been marked by the integration of advanced technologies and methodologies in forensic accounting practices, reshaping the way financial fraud is detected and investigated. However, the research was conducted in the United States whereas the research at hand was done in Kenya. This study presented a contextual gap as the current study focuses on ICT integration in collecting, examining, processing, and preserving fraud evidence on the performance of fraud investigators.

Button et al. 2022) in a study on the assessment of the seriousness of cybercrime with a focus on the perspective of victims of crimes related to computer misuse in the UK indicated that the victims of cybercrime in the UK were not likely to repost crimes immediately due to the perception that law enforcement was not well resourced to handle these types of offenses. Parpworth et al. (2022) further indicate that the police struggle to surmount the practical and legal difficulties in the process of cybercrime identification as they try to cope with the technological advancements as well as the jurisdictional issues and geographical locations of fraud suspects and victims. The study presents both conceptual and contextual gaps as the current study focuses on ICT integration in collecting, examining, processing, and preserving fraud evidence on the performance of fraud investigators in Kenya.

Focusing on the Kenyan context, a study by Okemwa and Nasieku (2023) on the effect of forensic fraud investigation on the financial performances of sugar processing firms in western Kenya indicates that Kenya has witnessed huge economic fraud and crime cases including Afya House scandal, NYS and Eurobond which led to losses of large sums of money. This highlights the failure of the conventional audit approach to fight fraud, which necessitates a more refined approach to curb these vices including the integration of information communication technology. However, no study has been done on the integration of ICT into the performance of fraud investigators by the directorate of criminal investigations officers hence presenting a knowledge/ empirical gap that the study at hand seeks to fill.

Objectives of the Study

The following objectives guided the study.

i. To examine the effect of ICT in collecting Fraud evidence on the performance of fraud investigators within the DCI, Kenya.

ii. To examine the effect of ICT in examining fraud evidence on the performance of fraud investigators within the DCI, Kenya.

LITERATURE REVIEW

The study is guided by anchorage theories and empirical literature which are discussed in detail in the next sections.

Theoretical Literature Review

The theories guiding the study included technology acceptance model and the diffusion of innovation theory.

Diffusion of Innovation Theory

The theory was postulated by E.M. Rogers in 1962 and provides a description of the speed and pattern at which practices, new products, and ideas spread through the population. The spread works better with behavioural adoption rather than prevention or cessation of behaviours. However, the theory does not take into account the resources or the social support of an individual to support the new innovation or behaviour (Haider & Kreps, 2004). Furthermore, the observations we make from organizations and individuals when they make decisions regarding the adoption of innovations are not adequately covered by the theory (George et al., 2012).

The theory further fails to give clear operational and conceptual definitions of adoption. It also fails to differentiate between the adoption of innovation at the individual, user level and the authorization/acquisition of an innovation at the level of an organization (Theingi *et al.,* 2017). The theory further fails to specify theoretical adoption, support, and the effects of mandates on diffusion through adequate research designs. According to the theory, innovation is associated with features that are measurable and distinct even though technologies are not discrete packages (Lyytinen & Damsgaard, 2001). Other critics of the theory indicate that technologies do not diffuse in a homogenous and fixed social ether and that the rate of diffusion is not solely a function of push and pull forces. Critics further indicate that choices are not functions of adopter's properties, preference functions, and available information (Lorey *et al.,* 2022).

The theory is significant in the study of ICT integration and the performance of fraud investigators in Kenya. This is because, with the rapid developments in technological innovations, advancements in fraud commission have also been witnessed as the fraudsters have been applying technology in committing fraud. Similarly, fraud investigators have also relied on technology to make the process of investigating fraud efficient and effective to enhance evidence for the purpose of litigation.

Technology Acceptance Model

Fred Davis (1986) postulated the model considered as one of the most influential technology acceptance models. The model exhibits two main features that influence technological adoption by individuals. These include perceived technological ease of use as well as its usefulness, which are considered the main factors influencing individual's attitude towards adopting new technology. The technology acceptance model has been criticized by a number of scholars. Ajibade, (2018) indicated that the model is not practically applicable or suitable to companies and other organizations such as libraries with regulations and rules but is suitable for use by individuals. Furthermore, there are inadequacies in the application of the model by the SMEs in information adoption. The model cannot give full explanations of the reasons behind the use and acceptance of technology in the business environment. In addition, the model may have been designed for personal use technology purposes and has not been designed for business or institutional context of application (Ajibade, 2018).

The technology acceptance model has also been criticized as it takes into account criticism of triviality, foretelling capability, restricted descriptive capability, contentious heuristic value, and short of any practical value. The model is incapable of taking into account other considerations including structural imperatives and cost that are significant in the development of innovation (Raji *et al.,* 2022). The model further applies measures such as interpersonal influence and behavioural intention that are subjective, which may include norms, values, or personal attributes (Malatji *et al.,* 2020).

The theory is revenant to the study of ICT integration and performance of fraud investigators in Kenya. This is because of the advancements in technological innovations, fraudsters are finding technology an easy avenue to commit crimes and to conceal evidence. In the same case, the fraud investigators also find efficiency and effectiveness in the application of technology in their processes in fraud investigations. Thus, the theory was useful to the current study.

Empirical Literature Review

Performance of Fraud Investigators

A research study was carried out by Ramadhan (2023) on analyzing performance anomaly and the profiles of fraudsters for fraud detection and prevention. From the results, staff with single marital status and very high category are potential red flags for fraud perpetrators. The other category of employees who are potentially considered as red flags for fraud perpetration are the youthful employees aged between 30 to 35 years with 3 to 5 years of service. Interpersonal approach can be mixed with the utilization of technology in analyzing fraud perpetration.

Sadgali et al. (2019) carried out an investigation with a focus on the performance of the techniques of machine learning in financial fraud detection. The study indicated that as a result of financial fraud, the financial sector faces serious consequences. Thus, it is imperative that the financial sector ought to continuously improve its fraud detection systems. Fraud can have negative effects on the cost of living, destabilize savings, and can reduce confidence in the industry. Even though financial institutions utilize different fraud prevention models, fraudsters are also innovative as they also device ways of intruding such protective systems. Financial fraud continues to be witnessed in spite of the continued efforts by government, law enforcement as well as the financial institutions to address the problem. Fraudsters tend to be a fast, intelligent, and very inventive fraternity.

In a study on rule-based machine learning for fraud detection, Islam et al. (2024) pointed out that even though security and preventative precautions are implemented to reduce the incidences of fraud, fraudsters are constantly innovating ways of evading security systems. There is a significant challenge posed by the existing models for classifying transactions into either fraudulent or legitimate transactions based the datasets that are highly imbalanced. A variety of metrics are adopted in assessing the effectiveness of the rule-based model including receiver characteristic values, Mathew's correlation coefficient, confusion matrix, recall, precision, specificity, and accuracy.

Novita and Anissa (2022) in a study on data analytics role for detecting indications of fraud in the Indonesian public sector did indicate a positive and significant effect of the adoption of data analytics in the public sector in Indonesia in detecting indications of fraud. Data analytics makes it easier to audit evidence collection, do an analysis of data, and determine likely risks that may have occurred or would occur and hence are helpful to the public sector examiners in the audit process. Since data is considered an asset for every organization and hence data analytics serves to maintain the security of data. In maintaining transparent report results in the existing conditions, the Indonesian public sector has adopted data analytics, which is essential in making real-time decisions.

In a study on the introduction of artificial intelligence and its significance to the management of modern business, Thakur (2024) underscored that the new forms of fraudulent activities have been catalyzed by the increased digital adoption and hence effective management of fraud is essential to enhance growth and market the expectations of customers for digital experiences. Within the new approach, a best-practice fraud model is combined with the considerations of customer experience to achieve a balance among several goals including new business values, improved customer experience, optimization of costs, customer protection, and loss prevention. Thus, there is a need for organizations to consider customer experience, fraud management, and authentication simultaneously.

Jillo (2017) carried out research at the fraud investigation unit on the effectiveness of fraud control at the Central Bank of Kenya using a descriptive research design and questionnaires as well as interviews as the sources of primary data. From the results, insufficient sentences awarded by the courts to the convicts and the legal constraints were found. Furthermore, successful investigations of bank fraud were found to be hindered by the laws present in the constitution of Kenya 2010 that provide for customer confidentiality and protect witnesses in fraud cases, lack of IT reports, time constraints in carrying out forensic investigations, and delays in obtaining specialist reports in the banks.

Effect of ICT in Collecting Fraud Evidence on the Performance of Fraud Investigators

Studies have been conducted around this area of study. A research study was carried out by Hussaini et al. (2021) on how information and communication influence the detection and prevention of fraud in Nigerian deposit money banks. Simple random sampling was employed and the outcomes indicated that efficient fraud disclosure, effective monitoring, fraud investigation, effectiveness of communication, and adequate quality of information positively and significantly affected the detection of fraud in the deposit money banks in Nigeria.

Abiola (2013) carried out a research study on ICT impacts on the prevention and detection of internal controls of fraud. In the analysis of quantitative data, the study adopted one-way ANOVAs, correlation coefficients, and cross tabulations while the qualitative analysis made use of thematic analysis. From the results, the IT-based techniques and tools have had positive effects on the objectivity and independence of the internal auditors and hence the auditors are continuously adopting them. The results further indicated that the techniques and tools are efficient in electronic fraud detection and hence the likelihood of preventing fraud. Further, other than being effective in preventing fraud, continuous online auditing is not suited for fraud detection in the financial business.

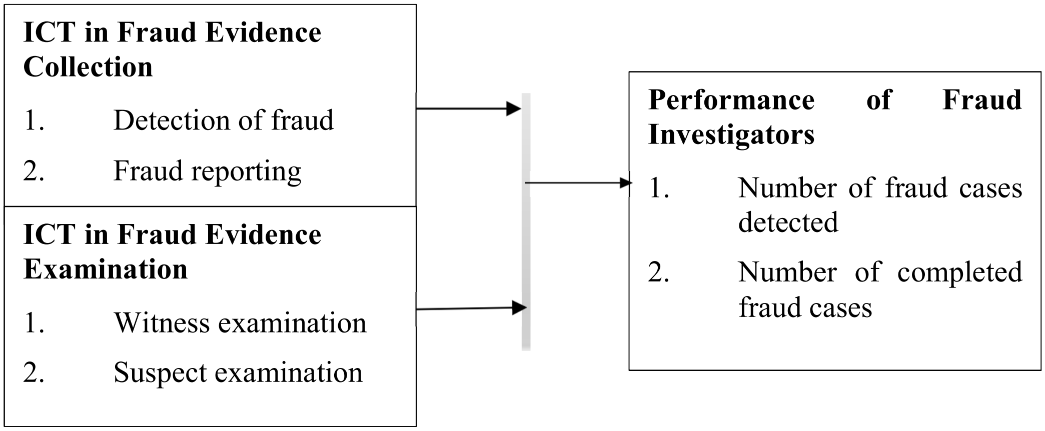
In Nigeria, research done by Akinbowale (2018) on information communication technology effects on forensic accounting indicated the presence of credible evidence showing that IT-based forensic accounting would significantly bring about a speedy process where relevant information is generated to serve as evidence to support fraudulent cases. However, the study did not find any evidence indicating that evidence accuracy significantly relates to investigation using ICT facilities.

A study was conducted by Adam and Fazekas (2021) on whether emerging technologies help in the successful fight against corruption. The research study indicated that ICT is viewed as a positive tool for making governments less corrupt, accountable, and more transparent.

However, the evidence to support this is often misunderstood and mixed. ICT can support anticorruption by influencing public scrutiny through government-citizen interactions, facilitating citizen participation, promoting accountability and transparency, and facilitating reporting of corruption. However, ICT can also facilitate corruption through the misuse of technologies, cryptocurrencies, and the dark web.

Mwai et al. (2023) carried out a study on ICT risk management and its role in insider fraud prevention in commercial banks in Nairobi County. The study used an explorative research design and inferential statistics were adopted. From the findings, there was a positive insignificant correlation between information security implementation, ICT awareness, and ICT risk assessment. However, information security audits and insider fraud prevention significantly and positively correlated. Thus, information security implementation, ICT awareness, and ICT risk assessment are significant in preventing commercial bank insider fraud.

Conceptual Framework


ICT in Fraud Evidence Collection
1. Detection of fraud
2. Fraud reporting
ICT in Fraud Evidence Examination
1. Witness examination
2. Suspect examination
Performance of Fraud Investigators
1. Number of fraud cases detected
2. Number of completed fraud cases

RESEARCH METHODOLOGY

The study adopted a descriptive research design that gives a description of how things relate to each other and as they naturally occur. Thus, it is suitable for describing the effect of ICT on fraud investigators, performance in Kenya. The study was conducted at the DCI headquarters, Kiambu Road, Kenya. The investigation covered the units; Bank Fraud Investigation Unit, Insurance Fraud Investigations Unit, Sacco Fraud Investigations Unit, Economic and Commercial Crimes Unit, Capital Markets Fraud Investigations Unit, and Cybercrime Investigations Unit of DCI. DCI headquarters, Kiambu Road has been chosen because complex fraud cases are handled by the officers at the headquarters.

The respondents were drawn from the Bank Fraud Investigation Unit, Insurance Fraud Investigations Unit, Sacco Fraud Investigations Unit, Economic and Commercial Crimes Unit, Capital Markets Fraud Investigations Unit, and Cybercrime Investigations Unit of the Directorate of Criminal Investigations. Though Sacco Fraud Investigations Unit is based at

Sacco Societies Regulatory Authority (SASRA) offices, Insurance Fraud Investigations Unit is based at Insurance Regulatory Authority offices, Bank Fraud Investigation Unit, seconded under the Central Bank of Kenya with offices at Ex-telecoms building Nairobi and Capital Markets Fraud Investigations Unit with offices at Embankment Plaza Upper hill Nairobi all report to DCI Headquarters, Kiambu Road on all reports regarding the findings and operations of fraud cases under investigation. Economic and Commercial Crimes Unit and Cybercrime Investigations Unit are domiciled at DCI. A representative sample of 234 respondents was scientifically selected using the Yamane (1985) formula. The study used questionnaires that contained both open and closed-ended questions in data collection. Collected data was analyzed using descriptive statistics including, frequencies and percentages.

RESULTS AND FINDINGS

A total of 234 respondents were contacted to participate in the study. However, 166 questionnaires were dully filled and collected back representing 70.9% response. Data on gender showed that 88% of the respondents were male whereas 12% were female. Thus, majority of the respondents were male. Data on departments that respondents were drawn showed that 18.1% of the respondents were working at cybercrime investigation department, 15.7% were working at insurance fraud department, 15.1% were working at financial investigation unit and 13.9% stationed at economic and commercial crimes unit. In addition, 13.3% working at Sacco fraud department, 12% were working at bank fraud investigation unit and finally, 9.6% of the respondents were working at capital markets fraud investigations unit. 2.4% of the respondents did not indicate their departments.

Data on the highest level of education attained showed that the majority (60%) of the participants had university education as their highest level of education, 27.7% had college as their highest level of education whereas 11.4% had secondary education as their highest educational qualification. Hence, most of those contacted had a university education as their highest education level.

Data on the period that the respondents had worked in their current departments indicated that the majority of the participants had been serving in their current departments for between 5 and 10 years whereas 27.1% of the respondents had served in their current departments for between 2 and 5 years. In addition, 25.9% had served in their current departments for more than 10 years and finally, 7.2% had been serving in their present departments for less than 2 years. This is a sign that the majority of the respondents had been serving for more than 2 years in their current departments.

Data on the Integration of ICT in Fraud Investigation showed that the majority (97.6%) of the respondents indicated that ICT had been intergraded in fraud investigation whereas 2.4% recorded a contrary opinion.

Integration of ICT in Fraud Evidence Collection

The objective of the research was to determine the effect of the integration of ICT in fraud evidence collection on the performance of fraud investigators. The analysis involved descriptive statistics as well as correlation and regression results.

Results of ICT in collecting Fraud evidence on the performance of fraud investigators

The study used primary data that was collected using questionnaires. A five-point Likert Scale was also used. The respondents were asked to indicate their level of agreement with regard to the statements presented to them. The descriptive outcomes from the analysis of the data on the integration of ICT in fraud evidence collection are presented in the subsequent section.

Table 1: Descriptive Results for ICT Integration in Fraud Evidence Collection

	SD	D	N	A	SA		
	n %	**n %**	**n %**	**n %**	**n %**	**M**	**S Dev**
ICT has been adopted in our department to detect fraud	9 5.4%	13 7.8%	21 12.7%	66 39.8%	57 34.5%	3.9	1.1
With ICT, there has been enhanced efficiency in fraud detection	10 6%	6 3.6%	20 12%	64 38.6%	66 39.8%	4.0	1.1
ICT has made it easy for fraud reporting	8 4.8%	9 5.4%	24 14.5%	56 33.7%	69 41.6%	4.0	1.1
There has been increased fraud reporting as a result of the integration of ICT	10 6%	10 6%	32 19.3%	58 34.9%	56 33.7%	3.8	1.1
ICT has enhanced secrecy and privacy for the persons reporting fraud	11 6.6%	7 4.2%	28 16.9%	51 30.7%	69 41.6%	4.0	1.2
With ICT integration, there has been timely fraud reporting	5 3%	15 9%	22 13.3%	65 39.2%	59 35.5%	4.0	1.1
Aggregate Mean and Standard Deviation						**4.0**	**1.1**

The descriptive results of the integration of ICT in fraud collection indicate that there was concurrence among the responses with an SD of 1.1 and a mean of 3.9 that ICT has been adopted in their department to detect fraud. The statement, with ICT, there has been enhanced efficiency in fraud detection recorded a mean and SD of 4.0 and 1.1 implying an agreement on average. The responses were also in tandem on average with a mean and SD of 4.0 and 1.1 that ICT has made it easy for fraud reporting. The statement, there has been increased fraud reporting as a result of the integration of ICT attracted a mean of 3.8 and SD of 1.1 implying a concurrence on average. The responses were in concurrence with an average of 4.0 and SD of 1.2 that ICT has enhanced secrecy and privacy for the persons reporting fraud. Finally, the statement, with ICT integration, there has been timely fraud reporting recorded a mean and respective SD of 4.0 and 1.1 respectively implying that the responses were in tandem on average.

Correlation results of ICT in collecting Fraud evidence on the performance of fraud investigators

This section presents the analysis to determine the direction and magnitude of the association between ICT integration in fraud evidence collection and the performance of fraud investigators. The values obtained from the analysis of correlation analysis ranged between +1 and -1 whereby +1 pointed out the presence of perfect correlation whereas -1 represented negative correlation and 0.000 for no correlation. The range of values between 0.001 to 0.250 indicated the presence of a weak correlation between the variables and a correlation that is moderately strong represented by a range from 0.251 to 0.500. Further, any value between *0.751 to 0.999 indicated a strong correlation between the variables.*

Table 2: Correlation Results of ICT Integration in Fraud Evidence Collection and Performance

		Performance	**Fraud Evidence Collection**
Performance	Pearson Correlation	1	
	Sig. (2-tailed)		
	N	166	
Fraud Evidence Collection	Pearson Correlation	.568**	1
	Sig. (2-tailed)	0.000	
	N	166	166

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

The outcomes point out that, the correlation between ICT integration in fraud evidence collection and the performance of fraud investigators was strong and positive and significant ($r = 0.568$, $p = 0.000 < 0.01$). This implies that the integration of ICT in fraud evidence collection is a significant determinant of the performance of fraud investigators. The results are in tandem with the findings of Abiola (2013) which pointed out that the IT-based techniques and tools have had positive effects on the objectivity and independence of the internal auditors and hence the auditors are continuously adopting them. The results further indicated that the techniques and tools are efficient in electronic fraud detection and hence the likelihood of preventing fraud. On the other hand, other than being effective in preventing fraud, continuous online auditing is not suited for fraud detection in the financial business.

Regression of results of ICT in collecting Fraud evidence on the performance of fraud investigators

Simple linear regression analysis was conducted to determine the linear relationship between the variables in the study that is ICT integration in fraud evidence collection and the performance of fraud investigators. The estimated model was;

$$\mathbf{Y = \beta_0 + \beta_1 X_1 + \varepsilon}$$

Where,

Y is the performance of fraud investigators, β_0, β_1, are constant terms, X_1 represents the integration of ICT in collecting fraud evidence, ε represents the error term.

Table 3: Model Summary

R	R Square	Adjusted R Square	Std. Error of the Estimate
.568a	0.322	0.318	0.73572

It can be noted that the R Square value for the estimated model was 0.322. This implies that the integration of ICT in fraud evidence collection explains to a tune of 32.2% of the variations in the performance of fraud investigators. Thus, the integration of ICT in fraud evidence collection is a significant determinant of the performance of fraud investigators.

Table 4: ANOVA

	Sum of Squares	df	Mean Square	F	Sig.
Regression	42.185	1	42.185	77.935	.000b
Residual	88.771	164	0.541		
Total	**130.956**	**165**			

From the results presented, the reported p value (0.000<0.05) implies that the estimated model is statistically significant. The significance of the model is further supported by the calculated F value 77.935 higher than the F critical value.

Table 5: Regression Coefficient

	Unstandardized Coefficients		Standardized Coefficients	T	Sig.
	B	Std. Error	Beta		
(Constant)	2.138	0.214		9.997	0.000
Fraud Evidence Collection	0.47	0.053	0.568	8.828	0.000

The estimated model was;

$Y = 2.138 + .47X_1$

Where,

Y is performance of fraud investigators,

X_2 represents integration of ICT in collecting fraud evidence.

The coefficient of integration of ICT in collecting fraud evidence was positive (0.47) and significant statistically (0.000<0.05). Therefore, a unit enhancement in the integration of ICT in collecting fraud evidence would yield a significant 0.47 units improvement in the performance of fraud investigators. Thus, the study concludes that the integration of ICT in collecting fraud evidence is an important determinant of the performance of fraud investigators. The results of the study are in tandem with the findings of Hussaini et al. (2021) which indicated that efficient fraud disclosure, effective monitoring, fraud investigation, effectiveness of communication, and adequate quality of information positively and significantly affected the detection of fraud in the deposit money banks in Nigeria. The findings of Adam and Fazekas (2021) further indicated that ICT is viewed as a positive tool for making governments less corrupt, accountable, and more transparent. However, the evidence to support this is often misunderstood and mixed. ICT can support anticorruption by influencing public scrutiny through government-citizen interactions, facilitating citizen participation, promoting accountability and transparency, and facilitating corruption reporting. However, ICT can also facilitate corruption through the misuse of technologies, cryptocurrencies, and the dark web.

The findings of Mwai et al. (2023) however indicated that there was an insignificant positive correlation between information security implementation, ICT awareness, and ICT risk assessment. However, information security audits and insider fraud prevention significantly and positively correlated. Thus, information security implementation, ICT awareness, and ICT risk assessment are significant in preventing insider fraud in commercial banks.

Integration of ICT in Fraud Evidence Examination

The objective of the research was to determine the effect of the integration of ICT in fraud evidence examination on the performance of fraud investigators. The analysis involved descriptive statistics as well as correlation and regression results.

Results of ICT in examining fraud evidence on the performance of fraud investigators

The descriptive results from the analysis of the data on the integration of descriptive results from the analysis of the data on ICT integration in fraud evidence examination are outlined in the section that follows.

Table 6: Descriptive Results for ICT Integration in Fraud Evidence Examination

	SD	D	N	A	SA		
	n %	n %	n %	n %	n %	M	S Dev
With the integration of ICT, fraud witnesses do not have to personally present themselves for examination	12 7.2%	8 4.8%	29 17.5%	61 36.7%	56 33.7%	3.8	1.2
ICT has made the process of witness examination efficient	10 6.1%	8 4.8%	22 13.3%	57 34.5%	68 41.2%	4.0	1.1
ICT integration has enhanced the security of witnesses	10 6%	7 4.2%	25 15.1%	62 37.3%	62 37.3%	4.0	1.1
ICT integration has made fraud suspect examination efficient	8 4.8%	7 4.2%	32 19.3%	69 41.6%	50 30.1%	3.9	1.0
With the integration of ICT, the quality of suspect examination has been enhanced	13 7.8%	5 3%	19 11.4%	76 45.8%	53 31.9%	3.9	1.1
ICT examination has improved the quality of evidence gathered from fraud suspects and witnesses	11 6.6%	5 3%	18 10.8%	67 40.4%	65 39.2%	4.0	1.1
Aggregate Mean and Standard Deviation						**3.9**	**1.1**

The descriptive results of the integration of ICT in fraud examination indicate that there was concurrence among the responses with a mean of 3.8 and an SD of 1.2 that with the integration of ICT, fraud witnesses do not have to personally present themselves for examination. The statement, ICT has made the process of witness examination efficient recorded a mean and SD of 4.0 and 1.1 implying a concurrence on average. The responses were also in tandem on average with a mean and SD of 4.0 and 1.1 that ICT integration has enhanced the security of witnesses. The statement, ICT integration has made fraud suspect examination efficient recorded a mean of 3.9 and SD of 1.0 implying that the responses were in tandem on average. The responses were in concurrence with a mean of 3.9 and SD of 1.1 that with the integration of ICT, the quality of suspect examination has been enhanced. Finally, the statement, ICT examination has improved the quality of evidence gathered from fraud suspects and witnesses recorded a mean and respective SD of 4.0 and 1.1 respectively implying concurrence on average.

Correlation results of ICT in examining fraud evidence on the performance of fraud investigators

This section presents the analysis to determine the magnitude and direction of the association between ICT integration in fraud evidence examination and the performance of fraud investigators. The values obtained from the analysis of correlation analysis ranged between +1 and -1 whereby +1 pointed out the presence of perfect correlation whereas -1 represented negative correlation and 0.000 for no correlation. The range of values between 0.001 to 0.250 indicated the presence of a weak correlation between the variables and a correlation that is moderately strong represented by a range from 0.251 to 0.500. Further, any value between 0.501 to 0.750 indicated a strong correlation between the variables. Values between 0.751 to 0.999 indicated a very strong variable correlation.

Table 7: Correlation Results of ICT Integration in Fraud Evidence Examination and Performance

		Performance	**Fraud Evidence Examination**
Performance	Pearson Correlation	1	
	Sig. (2-tailed)		
	N	166	
Fraud Evidence Examination	Pearson Correlation	.546**	1
	Sig. (2-tailed)	0.000	
	N	166	166

From the results, the correlation between ICT integration in fraud evidence examination and performance of fraud investigators was strong and positive and significant (r = 0.546, p = 0.000<0.01). This implies that the integration of ICT in fraud evidence examination is a significant determinant of the performance of fraud investigators. The results concur with the findings of Akinbowale (2018) which pointed out the presence of credible evidence showing that IT base forensic accounting would significantly bring about a speedy process where relevant information is generated to serve as evidence to support fraudulent cases. However, the study did not find any evidence indicating that evidence collection accuracy has a significant relationship with carrying out an investigation using ICT facilities.

Regression of results of ICT in examining fraud evidence on the performance of fraud investigators

Simple linear regression analysis was conducted to determine the linear relationship between the variables in the study that is ICT integration in fraud evidence examination and the performance of fraud investigators. The estimated model was;

$\mathbf{Y = \beta_0 + \beta_2 X_2 + \varepsilon}$

Where,

Y is the performance of fraud investigators, β_0, β_2 are constant terms, X_2 represents the integration of ICT in examining fraud evidence, ε represents the error term.

Table 8: Model Summary

R	R Square	Adjusted R Square	Std. Error of the Estimate
.546a	0.298	0.293	0.74887

An R square of 0.298 implies that the integration of ICT in fraud evidence examination explains a total of 29.8% of the changes in the performance of fraud investigators. Thus, the integration of ICT in fraud evidence examination is a significant determinant of the performance of fraud investigators.

Table 9: ANOVA

	Sum of Squares	df	Mean Square	F	Sig.
Regression	38.985	1	38.985	69.517	.000b
Residual	91.971	164	0.561		
Total	**130.956**	**165**			

From the results presented, the reported p-value (0.000<0.05) implies that the estimated model is statistically significant. The significance of the model is further supported by the calculated F value 69.517 higher than the F critical value.

Table 10: Regression Coefficient

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	2.394	0.196		12.194	0.000
Fraud Evidence Examination	0.418	0.05	0.546	8.338	0.000

The estimated model was;

$\mathbf{Y = 2.394 + .418X_2}$

Where,

Y is the performance of fraud investigators,

X_2 represents the integration of ICT in examining fraud evidence.

The coefficient of integration of ICT in examining fraud evidence was significant statistically (0.000<0.05) and positive (0.418). Therefore, a unit improvement in the integration of ICT in examining fraud evidence would yield a significant 0.418 units improvement in the performance of fraud investigators. Thus, the study concludes that the integration of ICT in examining fraud evidence is a significant determinant of the performance of fraud investigators. The results concur with the findings of Akinbowale et al. (2024) which postulated that the mix of external and internal technologies for fighting fraud including data mining, digital analysis, financial ratios, virus protection, discovery sampling, continuous auditing, encryption, firewalls, and filtering software results in a positive effect on the mitigation of cyber fraud. Furthermore, Button and Cross (2017) indicated that crime prevention and enhanced security have contributed to the decline in crime and reduced opportunities for crime. Cases of traditional crimes have declined because of technological revolution. Globally, the high levels of fraud victimization because of cyber-attacks have been ill-equipped to capture and hence have further made the problem worse. The desire by the fraudsters to engage in fraud has not been changed by the evolution of technology but rather, the technological advancement has changed how crime is committed. The outcomes also concur with the findings of Mosoti et al. (2022) which pointed out that forensic auditing and investigation techniques were applied by the institutions under study to fight fraud. As a result, the institutions witnessed a decline in the incidences of fraud hence contributing positively to the financial performance of the institutions. Thus, forensic auditing and investigation techniques had a significant positive relationship with financial performance.

CONCLUSIONS AND RECOMMENDATIONS

Conclusion

Conclusions were made as per the objectives. The investigation concludes that the integration of ICT in the collection of fraud evidence has a significant positive effect on the performance of fraud investigators. ICT can support anticorruption by influencing public scrutiny through government-citizen interactions, facilitating citizen participation, promoting accountability and transparency, and facilitating reporting of corruption. However, ICT can also facilitate corruption through the misuse of technologies, cryptocurrencies, and the dark web. Information security implementation, ICT awareness, and ICT risk assessment are significant in preventing fraud. Efficient fraud disclosure, effective monitoring, fraud investigation, effectiveness of communication, and adequate quality of information positively and significantly affect the detection of fraud

The study concluded that the integration of ICT in the examination of fraud evidence has a positive and significant effect on the performance of fraud investigators. The mix of external and internal technologies for fighting fraud including data mining, digital analysis, financial ratios, virus protection, discovery sampling, continuous auditing, encryption, firewalls, and filtering software results in a positive effect on the mitigation of cyber fraud. Crime prevention and enhanced security have contributed to the decline in crime and reduced opportunities for crime. However, the desire by the fraudsters to engage in fraud has not been changed by the evolution of technology but rather; the technological advancement has changed how crime is committed.

Recommendations

The study recommends that the Directorate of Criminal Investigations ought to fully adopt technology in its process of collecting fraud in various departments. As technology advances, so do fraudsters. Therefore, the DCI should remain at the forefront of technological adoption for it to efficiently and effectively collect fraud evidence that can stand the test of litigation. The technology adoption should be included in the process of fraud evidence collection by making it easy for witnesses and suspects to record statements.

The Directorate of Criminal Investigations should also utilize technology in the examination of fraud evidence collected. Technological utilization makes it effective and efficient for the DCI officers to examine the evidence collected. This enhances the success of fraud investigation and consequently prosecution because technology would facilitate effective examination of fraud evidence that could successfully stand the test of litigation.

REFERENCES

Abiola, J. (2013). The impact of information and communication technology on internal control's prevention and detection of fraud.

Adam, I., & Fazekas, M. (2021). Are emerging technologies helping win the fight against corruption? A review of the state of evidence. *Information Economics and Policy*, *57*, 100950.

Ajibade, P. (2018). Technology acceptance model limitations and criticisms: Exploring the practical applications and use in technology-related studies, mixed-method, and qualitative researches. *Library Philosophy and Practice*, *9*.

Akinbowale, O. E. (2018). Information communication technology and forensic accounting in Nigeria. *International Journal of Business and Finance Management Research*, *6*(1), 1-7.

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). An innovative approach in combating economic crime using forensic accounting techniques. *Journal of Financial Crime*, *27*(4), 1253-1271.

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2023). Application of forensic accounting techniques in the South African banking industry for the purpose of fraud risk mitigation. *Cogent Economics & Finance*, *11*(1), 2153412.

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2024). Investigating the level of effectiveness of the anti-fraud technologies employed by the South African banking industry for cyberfraud mitigation. *Journal of Financial Crime*, *31*(1), 201-225.

Akinbowale, O. E., Mashigo, P., & Zerihun, M. F. (2023). The integration of forensic accounting and big data technology frameworks for internal fraud mitigation in the banking industry. *Cogent Business & Management*, *10*(1), 2163560.

Alastal, A. I., & Shaqfa, A. H. (2023). Enhancing Police Officers' Cybercrime Investigation Skills Using a Checklist Tool. *Journal of Data Analysis and Information Processing*, *11*(2), 121-143.

Alberus, R. W. (2019). Translating a Digital Strategy for South Africa's Police Services.

Apau, R., & Koranteng, F. N. (2020). An overview of the digital forensic investigation infrastructure of Ghana. *Forensic Science International: Synergy*, *2*, 299-309.

Baz, R., Samsudin, R. S., & Che Ahmad, A. (2017). The impact of external factor on bank fraud prevention and the role of capability element as moderator in Saudi Arabia banking sektor. *Asian Academic Research Journal of Social Sciences & Humanities*, *4*(3), 139-148.

Burns, R., & Burns, R. P. (2008). Business Research Methods and Statistics Using SPSS: What, Why and How? *Business Research Methods and Statistics Using SPSS*, 1-560.

Button, M., & Cross, C. (2017). Technology and Fraud: The 'Fraudogenic'consequences of the Internet revolution. In *The Routledge handbook of technology, crime and justice* (pp. 78-95). Routledge.

Button, M., Shepherd, D., Blackbourn, D., Sugiura, L., Kapend, R., & Wang, V. (2022). Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective. *Criminology & Criminal Justice*, 17488958221128128.

Chen, Y., & Wu, Z. (2022). Financial Fraud Detection of Listed Companies in China: A Machine Learning Approach. *Sustainability*, *15*(1), 105.

Dahabreh, I. J., & Hernán, M. A. (2019). Extending inferences from a randomized trial to a target population. *European journal of epidemiology*, *34*, 719-722.

Daraojimba, R. E., Farayola, O. A., Olatoye, F. O., Mhlongo, N., & Oke, T. T. (2023). Forensic Accounting In The Digital Age: A Us Perspective: Scrutinizing Methods And Challenges In Digital Financial Fraud Prevention. *Finance & Accounting Research Journal*, *5*(11), 342-360.

Dlamini, S., & Mbambo, C. (2019). Understanding policing of cybe-rcrime in South Africa: The phenomena, challenges and effective responses. *Cogent Social Sciences*, *5*(1), 1675404.

Fatoki, J. O. (2023). The influence of cyber security on financial fraud in the Nigerian banking industry. *International Journal of Science and Research Archive*, *9*(2), 503-515.

Felix, U. O. (2022). Evidence Collecting Processes and Fraud Examination: The Role of an Expert Forensic Accountant. *Asian Basic and Applied Research Journal*, 394-420.

Fysarakis, K., Lekidis, A., Mavroeidis, V., Lampropoulos, K., Lyberopoulos, G., Vidal, I. G. M., ... & Koufopavlou, O. (2023, July). PHOENI2X–A European Cyber Resilience Framework with Artificial-Intelligence-Assisted Orchestration, Automation & Response Capabilities for Business Continuity and Recovery, Incident Response, and Information Exchange. In *2023 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 538-545). IEEE.

George, G., McGahan, A. M., & Prabhu, J. (2012). Innovation for inclusive growth: Towards a theoretical framework and a research agenda. *Journal of management studies*, *49*(4), 661-683.

Gisairo, B. G. (2016). Effectiveness of use of biometric technology to curb fraud in medical insurance firms in Kenya (Doctoral dissertation, University of Nairobi).

Gottschalk, P. (2023). *Corporate compliance and conformity: A convenience theory approach to executive deviance*. Taylor & Francis.

Hagger, M. S. (2019). The reasoned action approach and the theories of reasoned action and planned behavior.

Haider, M., & Kreps, G. L. (2004). Forty years of diffusion of innovations: utility and value in public health. *Journal of health communication*, *9*(S1), 3-11.

Haq, M. A., Barthos, M., & Fakrulloh, Z. A. (2023, July). Digital Forensics in Online Fraud Crimes Investigation. In *ICLSSEE 2023: Proceedings of the 3rd International Conference on Law, Social Science, Economics, and Education, ICLSSEE 2023, 6 May 2023, Salatiga, Central Java, Indonesia* (p. 50). European Alliance for Innovation.

Hassan, S. Z., Salehi, P., Røed, R. K., Halvorsen, P., Baugerud, G. A., Johnson, M. S., ... & Sabet, S. S. (2022, June). Towards an AI-driven talking avatar in virtual reality for investigative interviews of children. In *Proceedings of the 2nd Workshop on Games Systems* (pp. 9-15).

Hooper, C., Martini, B., & Choo, K. K. R. (2013). Cloud computing and its implications for cybercrime investigations in Australia. *Computer Law & Security Review*, *29*(2), 152-163.

Hussaini, I., Aliyu, Y., & Bashir, A. B. (2021). Effect of Information and Communication on Fraud Prevention and Detection in Deposit Money Banks in Nigeria. *UMYU Journal of Accounting and Finance Research*, *1*(2), 21-30.

Islam, S., Haque, M. M., & Karim, A. N. M. R. (2024). A rule-based machine learning model for financial fraud detection. *International Journal of Electrical and Computer Engineering (IJECE)*, *14*(1), 759-771.

Jillo, H. Q. (2017). *Effectiveness of Fraud Control at the Banking Fraud Investigation Unit at the Central Bank of Kenya* (Doctoral dissertation, University of Nairobi).

Kafteranis, D., Turksen, U., & Sachoulidou, A. (2023). Artificial Intelligence in Law Enforcement Settings: AI Solutions for Disrupting Illicit Money Flows.

Kim, S., Jeong, S. H., & Hwang, Y. (2013). Predictors of pro-environmental behaviors of American and Korean students: The application of the theory of reasoned action and protection motivation theory. *Science Communication*, *35*(2), 168-188.

Levi, M. (2017). Organized fraud and organizing frauds: Unpacking research on networks and organization. In *Transnational Financial Crime* (pp. 309-340). Routledge.

Lord, N., & Levi, M. (2023). Economic crime, economic criminology, and serious crimes for economic gain: On the conceptual and disciplinary (dis) order of the object of study. *Journal of Economic Criminology*, *1*, 100014.

Luther, K., Arenzon, V., Curtis, A., de Almeida, H., Hachey, J., & Lundy, J. (2024). Do Automated and Virtual Interrogation and Deception Detection Systems Work?. In *The Impact of Technology on the Criminal Justice System* (pp. 3-40). Routledge.

Lyytinen, K., & Damsgaard, J. (2001). What's wrong with the diffusion of innovation theory? The case of a complex and networked technology. In *Diffusing Software Product and Process Innovations: IFIP TC8 WG8. 6 Fourth Working Conference on Diffusing Software Product and Process Innovations April 7–10, 2001, Banff, Canada 4* (pp. 173-190). Springer US.

Malatji, W. R., Eck, R. V., & Zuva, T. (2020). Understanding the usage, modifications, limitations and criticisms of technology acceptance model (TAM). *Advances in Science, Technology and Engineering Systems Journal*, *5*(6), 113-117.

Maluleke, W. (2023). Exploring Cybercrime: An Emerging Phenomenon and Associated Challenges in Africa. *International Journal of Social Science Research and Review*, *6*(6), 223-243.

Mandal, A. (2023). Fathoming fraud: unveiling theories, investigating pathways and combating fraud. *Journal of Financial Crime.*

Mat Ridzuan, N. I., Said, J., Razali, F. M., Abdul Manan, D. I., & Sulaiman, N. (2022). Examining the Role of Personality Traits, Digital Technology Skills and Competency on the Effectiveness of Fraud Risk Assessment among External Auditors. *Journal of Risk and Financial Management*, *15*(11), 536.

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: Evidence from seven nations. *Computers & Security*, *120*, 102820.

Mosoti, J. M., Wafula, J., & Nyang'au, A. (2022). Effect of Forensic Auditing and Investigation Techniques on the Financial Performance of Deposit-Taking Microfinance Institutions in Kenya. *Internatio;nal Research Journal of Business and Strategic Management*, *4*(3).

Mugisha, D. (2019). Role and impact of digital forensics in cyber-crime investigations. *International Journal of Cyber Criminoligy*.

Musyoki, K. M. (2023). Internal Control Systems and their role in Financial Fraud Prevention in Kenya. *African Journal of Commercial Studies*, *3*(3), 173-180.

Mwai, R., Wabala, S., & Ogada, K. (2023). Role of ICT Risk Management on Insider Fraud Prevention in Commercial Banks in Nairobi County. *International Journal of Technology and Systems*, *8*(2), 36-64.

National Police Service (2024). National Police Service. Available at https://www.nationalpolice.go.ke/2015-09-21-17-23-32/dci.html. Accessed on 31st January 2024.

Newman, W., Tshuma, Z., & Sitsha, L. (2023). An analysis of effects of forensic auditing in detecting fraud in state owned enterprises: a case study of ZESA.

Novita, N., & Anissa, A. I. N. A. (2022). The role of data analytics for detecting indications of fraud in the public sector. *International Journal of Research in Business and Social Science (2147-4478)*, *11*(7), 218-225.

Ohndyl G. O., Kimuyu J., & Sidha Z. (2023). Information Security Threats to e-government Services in Kenya. Global Journal of Human-Social Science: H Interdisciplinary, 23(7).

Okemwa, S., & Nasieku, T. (2023). Effect of Forensic Fraud Investigation on Financial Performances of Sugar Processing Firms in Western Kenya. *International Journal of Social Sciences and Information Technology*, 9(5) 2412-0294.

Oni, S., Berepubo, K. A., Oni, A. A., & Joshua, S. (2019, April). E-government and the challenge of cybercrime in Nigeria. In *2019 Sixth International Conference on e-Democracy & eGovernment (ICEDEG)* (pp. 137-142). IEEE.

Pace, D. S. (2021). Probability and non-probability sampling-an entry point for undergraduate researchers. *International Journal of Quantitative and Qualitative Research Methods*, *9*(2), 1-15.

Parpworth, N., Robinson, S., MacCulloch, R., Arentsen, V., White, V., Robinson, S., & Lawson, C. (2022). Theory, Practice and Principles. *Sage Journals*, 96(4). https://doi.org/10.1177/0032258X221107584.

Qonde, H. J. & Chepkonga, M. (2017). Effectiveness of Fraud Investigators at the Banking Fraud Investigation Unit, Central Bank of Kenya. *International Journal of Current Business and Social Sciences*, 1(7), 62-93.

Raji, I. D., Kumar, I. E., Horowitz, A., & Selbst, A. (2022, June). The fallacy of AI functionality. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (pp. 959-972).

Ramadhan, D. (2023). Analysis of Performance Anomaly and Fraudster Profile for Fraud Prevention and Detection. *Asia Pacific Fraud Journal*, *8*(2), 341-349.

Rashid, M. A., Al-Mamun, A., Roudaki, H., & Yasser, Q. R. (2022). An overview of corporate fraud and its prevention approach. *Australasian Accounting, Business and Finance Journal*, *16*(1), 101-118.

Sadgali, I., Sael, N., & Benabbou, F. (2019). Performance of machine learning techniques in the detection of financial frauds. *Procedia computer science*, *148*, 45-54.

Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, 100034.

Sileyew, K. J. (2019). Research design and methodology. *Cyberspace*, 1-12.

Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber, A., Badii, A., ... & Runevic, J. (2021). Follow the trail: Machine learning for fraud detection in Fintech applications. *Sensors*, *21*(5), 1594.

Sumirat, J. R. (2020). *Policing on Preventing Cyber Fraud in Indonesia* (Doctoral dissertation, Master Dissertation, University of York).

Thakur, R. (2024). Introduction to artificial intelligence and its importance in modern business management. In *Leveraging AI and emotional intelligence in contemporary business organizations* (pp. 133-165). IGI Global.

Theingi, T., Theingi, H., & Purchase, S. (2017). Cross-border remittance between emerging economies: an institutional perspective. *Journal of Business & Industrial Marketing*, *32*(6), 786-800.

Trafimow, D. (2009). The theory of reasoned action: A case study of falsification in psychology. *Theory & Psychology*, *19*(4), 501-518.

Van Dasselaar, T., Stewart, S. A., & Giddings, J. N. (2022). crime landscape.

Wicaksana, A. P., Kurnia, S., Ho, W., & Samson, D. (2021). The Role of Information Communication Technology in Mitigating Supply Chain Fraud. In *PACIS* (p. 151).

Xiuguo, W., & Shengyong, D. (2022). An analysis on financial statement fraud detection for Chinese listed companies using deep learning. *IEEE Access*, *10*, 22516-22532.