JURNAL LOCUS: Penelitian & Pengabdian
Volume 5 No. 10 October 2026, pp 9528-9546
E-ISSN 2829-7334
DOI: 10.58344/locus.v5i10.6471

The Influence of AI Readiness, Digital Forensic Competency, and Data Governance Practices on Fraud Detection Effectiveness among Certified Fraud Examiners in Zimbabwe: A Case of ACFE Zimbabwe Chapter 128

Joshua Foma[1]*, Tafadzwa Chimbare[2], Brian Marambo[3], Trust Chidadza[4], Rumbidzai Chibvongodze[5], Adiel Chikwekwete[6]
Universitas Indonesia, Indonesia[1]
Great Zimbabwe University, Zimbabwe[2]
Africa Research University, Zambia[3,6]
Midlands State University, Zimbabwe[4,5]
Email: joshua.foma@ui.ac.id*, tafadzwachimbare@gmail.com[2], marambobrian1@gmail.com[3], trustchidadza@gmail.com[4], rumbidzai06@yahoo.com[5], adielchikwekwete@gmail.com[6]

Keywords:
AI Readiness; Digital Forensic Competency; Data Governance; Fraud Detection Effectiveness; Certified Fraud Examiners.

This is an open access article under the CC BY-SA license.

Copyright © 2026 by Author. Published by Riviera Publishing

ABSTRACT

The digitalization of financial activities and the increasing complexity of technology-enabled fraud have required organizations to strengthen their fraud detection capabilities through technological adoption, professional expertise, and effective data governance. This study aimed to examine the influence of artificial intelligence (AI) readiness, digital forensic competency, and data governance practices on fraud detection effectiveness among Certified Fraud Examiners (CFEs) affiliated with the Association of Certified Fraud Examiners (ACFE) Zimbabwe Chapter 128. A quantitative approach with a cross-sectional survey design was employed. Data were collected from 117 respondents through an online questionnaire and analysed using descriptive statistics and multiple linear regression in IBM SPSS Statistics version 26. The results indicated that AI readiness had a positive but statistically insignificant association with fraud detection effectiveness ($\beta = 0.093$, $p = 0.186$). Digital forensic competency demonstrated a positive and statistically significant association ($\beta = 0.252$, $p < 0.001$), while data governance practices exhibited the strongest positive association ($\beta = 0.488$, $p < 0.001$). Collectively, the three predictors explained 58.9% of the variance in fraud detection effectiveness ($R^2 = 0.589$, $F = 54.073$, $p < 0.001$). These findings suggested that technological readiness alone was insufficient to enhance fraud detection effectiveness without adequate investigative competencies and robust data governance practices. Accordingly, organizations should adopt an integrated strategy that combines technological advancement, continuous digital forensic competency development, and strengthened data governance frameworks to improve fraud prevention and detection capabilities.

INTRODUCTION

The digitalization of financial activities has fundamentally transformed the nature of

fraud and the methods organizations employ to detect it (Chang et al., 2022; Daraojimba et al., 2023; Zhu et al., 2021). In the global business environment, integrated information systems, cloud computing, big data analytics, artificial intelligence (AI), digital payment platforms, and advanced analytical technologies are increasingly used to support financial transactions and oversight. These technological developments have improved operational efficiency, data processing speed, and large-scale analytical capabilities. However, digitalization has also created opportunities for fraud perpetrators to develop increasingly sophisticated, concealed, and technology-enabled fraudulent schemes. Consequently, conventional fraud detection approaches that rely primarily on manual verification, periodic audits, and traditional investigative procedures have become less effective in identifying anomalies within large datasets. Technologies such as big data analytics, cloud computing, AI, and advanced analytics enable organizations to process substantial volumes of information, identify suspicious transactions, and conduct more timely and accurate fraud investigations (Ikhsan et al., 2022; Mangala & Kumari, 2017; Sukardi, 2022). Furthermore, AI and machine learning have demonstrated the potential to improve fraud detection accuracy and reduce dependence on manual examination procedures (Ahmed et al., 2016; Ngai et al., 2011). Nevertheless, occupational fraud continues to impose substantial economic losses on organizations, emphasizing the importance of strengthening fraud prevention and detection capabilities (Association of Certified Fraud Examiners [ACFE], 2024).

Fraud detection effectiveness is influenced by several interconnected factors. The first is organizational readiness to adopt and utilize AI, commonly referred to as AI readiness. The availability of AI technologies does not necessarily translate into effective fraud detection without adequate technological infrastructure, qualified personnel, management support, organizational policies, financial resources, and training. Previous studies have identified financial constraints, limited technological expertise, and insufficient institutional support as significant barriers to AI adoption, particularly in developing economies (Dwivedi et al., 2021). The second factor is digital forensic competency. As financial transactions increasingly rely on electronic systems, fraud investigations require professionals capable of identifying, collecting, preserving, analysing, documenting, and presenting digital evidence in accordance with established forensic procedures and applicable legal requirements (Kranacher et al., 2022; Mabior & Wanyama, 2024; Siahaan et al., 2023). The third factor involves data governance practices, as analytical and investigative processes depend on data quality, security, integrity, completeness, and traceability. Inadequate data governance can compromise the reliability of investigative findings and increase the likelihood of erroneous decisions (Rikhardsson & Yigitbasioglu, 2018).

These factors may collectively influence fraud detection effectiveness. Organizations that adopt advanced analytical technologies without developing employees' ability to interpret analytical outputs may encounter difficulties converting technological findings into credible investigative evidence. Similarly, fraud examiners with advanced forensic expertise may face operational challenges when investigative data are incomplete, insecure, unverifiable, or insufficiently traceable. In this context, weak data governance practices may undermine the potential benefits of AI readiness and digital forensic competency because reliable data form the foundation of effective fraud analysis. Conversely, robust governance practices can

strengthen transparency, accountability, information integrity, internal controls, and fraud detection mechanisms (Andaru & Utami, 2024; Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2022). These challenges are particularly relevant in Zimbabwe, where resource constraints, weaknesses in financial crime detection systems, technological implementation barriers, and governance deficiencies have affected organizational responses to increasingly sophisticated financial crimes (Murinda & Chiwariro, 2023). Furthermore, successful fraud investigations depend not only on identifying suspicious transactions but also on the proper collection, preservation, analysis, documentation, and presentation of evidence that satisfies professional and legal standards (Murinda & Chiwariro, 2023; Mvunabandi, 2023).

This study examined three independent variables—AI readiness, digital forensic competency, and data governance practices—and one dependent variable, fraud detection effectiveness. AI readiness encompassed the technological and organizational capabilities required to adopt and utilize AI-based fraud detection systems, including technological infrastructure, technical expertise, organizational support, financial resources, training, and institutional policies (Dwivedi et al., 2021). Digital forensic competency reflected fraud examiners' professional capabilities in identifying, collecting, preserving, analysing, documenting, and presenting digital evidence in accordance with established forensic standards and applicable legal requirements (Kranacher et al., 2022; Mabior & Wanyama, 2024). Data governance practices encompassed organizational policies, procedures, controls, and accountability mechanisms intended to maintain data quality, integrity, security, accessibility, and traceability (Rikhardsson & Yigitbasioglu, 2018). Fraud detection effectiveness represented the ability of fraud examination processes to identify suspicious activities, investigate potential fraud, establish credible evidence, and support appropriate organizational responses.

The novelty of this study lay in integrating AI readiness, digital forensic competency, and data governance practices into a single quantitative research model examining fraud detection effectiveness among Certified Fraud Examiners (CFEs) affiliated with the Association of Certified Fraud Examiners (ACFE) Zimbabwe Chapter 128. Previous studies primarily examined AI adoption and organizational readiness independently, emphasizing analytical capabilities, operational efficiency, and technological implementation (Ahmed et al., 2016; Ngai et al., 2011). Other investigations concentrated on professional investigative competencies and digital forensic capabilities (Kranacher et al., 2022; Siahaan et al., 2023), while additional research emphasized data quality, internal controls, accountability, and evidence management (Rikhardsson & Yigitbasioglu, 2018). However, limited empirical research has simultaneously examined these three dimensions within an integrated framework for explaining fraud detection effectiveness. This research gap was particularly relevant in Zimbabwe, where previous investigations primarily addressed governance deficiencies, financial crime prevention, AI implementation challenges, and the legal admissibility of digital forensic evidence, with comparatively limited attention to the combined associations of AI readiness, digital forensic competency, and data governance practices among CFEs (Murinda & Chiwariro, 2023). Additionally, the study drew on the Unified Theory of Acceptance and Use of Technology (UTAUT; Venkatesh et al., 2003) and Fraud Pentagon Theory (Cressey,

1953; Mashitoh et al., 2023; Wolfe & Hermanson, 2004) to establish a conceptual framework connecting technological readiness, professional competency, organizational controls, and fraud detection effectiveness.

The urgency of this research stemmed from the widening gap between increasingly sophisticated digital fraud schemes and organizational capabilities to identify, investigate, and respond effectively to fraudulent activities. Although AI technologies offer substantial opportunities to enhance analytical capabilities and identify anomalous financial transactions, their effectiveness depends on professional expertise and reliable data governance practices that support the interpretation and application of analytical findings in fraud investigations. These concerns were particularly significant in Zimbabwe, where technological limitations, resource constraints, financial crime risks, governance challenges, and requirements for legally admissible evidence have presented substantial difficulties for fraud examination professionals (Murinda & Chiwariro, 2023). Organizations therefore need empirical evidence regarding whether AI readiness is independently associated with improved fraud detection effectiveness and how digital forensic competency and data governance practices contribute to investigative performance. Understanding these relationships is essential for establishing appropriate investment priorities, strengthening professional capabilities, and developing governance mechanisms capable of addressing technology-enabled financial crime. Accordingly, an integrated examination of these three factors could provide a stronger empirical foundation for organizational decision-making and the development of more effective fraud detection strategies.

Based on these considerations, this study aimed to examine the individual and combined associations of AI readiness, digital forensic competency, and data governance practices with fraud detection effectiveness among CFEs affiliated with ACFE Zimbabwe Chapter 128. Specifically, the study investigated the relationship between AI readiness and fraud detection effectiveness, assessed the contribution of digital forensic competency to investigative performance, examined the association between data governance practices and fraud detection effectiveness, and evaluated the collective explanatory power of the three independent variables. Through these objectives, the research sought to determine the extent to which technological readiness, professional forensic capabilities, and organizational data governance were associated with effective fraud detection. Furthermore, the study assessed whether the integrated model provided a more comprehensive explanation of variations in fraud detection effectiveness than the individual examination of each predictor.

This research was expected to provide theoretical, empirical, and practical contributions to fraud examination and organizational governance. Theoretically, it sought to extend the literature on fraud management, technology adoption, digital forensics, and data governance by integrating technological readiness, professional competency, and organizational controls within a unified analytical framework. Empirically, the study provided evidence from CFEs in Zimbabwe, contributing to a relatively underexplored context in fraud detection research. Practically, the findings were intended to assist ACFE Zimbabwe Chapter 128 and organizations employing fraud examination professionals in developing targeted competency enhancement programs involving AI applications, digital forensic investigations, and digital evidence management. The findings could also inform organizational investment decisions

concerning technological infrastructure, investigator training, and data governance improvements. For regulators and policymakers, the study offered insights into the importance of cybersecurity governance, professional competency standards, and effective data management frameworks in supporting fraud detection capabilities. Ultimately, the research sought to contribute to the development of a more integrated, evidence-based, and professionally credible approach to detecting and investigating technology-enabled financial crimes.

METHOD

Research Design and Strategy

This study employed a quantitative approach with a cross-sectional survey design to examine the associations of Artificial Intelligence (AI) Readiness, Digital Forensic Competency, and Data Governance Practices with Fraud Detection Effectiveness among Certified Fraud Examiners (CFEs) affiliated with the Association of Certified Fraud Examiners (ACFE) Zimbabwe Chapter 128. Data were collected during a single observation period using a structured questionnaire to assess the relationships among the predefined variables. The quantitative design enabled hypothesis testing through statistical analysis and the examination of the individual and combined contributions of the three independent variables to Fraud Detection Effectiveness (Creswell & Creswell, 2022).

Research Location and Context

The study was conducted within the professional context of ACFE Zimbabwe Chapter 128, with Certified Fraud Examiners as the primary unit of analysis. This context was chosen based on the characteristics of CFEs directly involved in fraud examinations, investigations, forensic analysis, and fraud prevention and detection activities. This professional environment was deemed suitable for analysing the three capabilities that were the focus of the study: readiness to use AI to support fraud detection, ability to handle digital evidence, and application of data governance in investigative activities. Although the study focused on a specific professional environment, respondents came from various organizational sectors, allowing the data to capture the variety of professional experiences and fraud examination practices in the Zimbabwean context. The study was conducted by collecting data at a single point in time, rather than through longitudinal observation, so the results obtained represent the relationships between variables based on the respondents' conditions during the study period (Creswell & Creswell, 2022).

Population and Research Sample

The study population was Certified Fraud Examiners in Zimbabwe, with particular attention to members affiliated with ACFE Zimbabwe Chapter 128. This population was selected because of their professional involvement relevant to fraud investigations, forensic examinations, evidence analysis, and other anti-fraud activities. The study obtained 117 complete responses, which were then used in the analysis. The sampling technique used a combination of purposive sampling and convenience sampling. Purposive sampling was used to ensure that individuals who became respondents had qualifications and professional experience in accordance with the research construct, while convenience sampling was used to gain access to members of the professional population who were available and willing to

participate in the study. The use of non-probability techniques was considered because a complete sampling frame was not available for the entire population of CFEs targeted by the study.

The adequacy of the number of respondents was checked using Green's (1991) guidelines for multiple linear regression analysis, namely $N \geq 50 + 8m$, where m represents the number of independent variables. Since the study had three independent variables, the minimum sample requirement was calculated to be $N \geq 50 + 8(3)$, resulting in a minimum requirement of 74 respondents. The final number of 117 respondents exceeded this limit and provided a more adequate basis for estimating regression coefficients and reduced the risk of estimation instability in models with multiple predictors. However, the use of non-probability techniques remains a consideration in interpreting the results because the study findings are not intended to be statistically representative of all fraud examination practitioners in Zimbabwe beyond the population participating in the study (Creswell & Creswell, 2022; Green, 1991; Hair et al., 2021).

Research Variables and Instruments

The research instrument is a structured questionnaire developed based on four main constructs: AI Readiness, Digital Forensic Competency, Data Governance Practices, and Fraud Detection Effectiveness. Each construct is measured using seven statements, resulting in a total of 28 main items. AI Readiness measures the readiness of technological infrastructure, AI skills, training, management support, AI integration in the fraud detection process, availability of financial resources, and organizational policies that support AI adoption. Digital Forensic Competency measures the ability to identify, collect, retain, analyse, document, and present digital evidence and the use of digital forensic tools. Data Governance Practices measures data quality and reliability, access control, audit trails, data policies, regulatory compliance, and information security. Fraud Detection Effectiveness measures detection accuracy, timeliness, investigative efficiency, reduction in fraud incidents, evidentiary capabilities, technological support for investigations, and successful prosecution.

All statements were measured using a five-level Likert scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, and 5 = Strongly Agree. This scale enabled respondents' professional perceptions of each aspect of the research to be transformed into quantitative data that could be compared and analysed statistically. The instrument was structured so that each construct had a set of indicators consistent with the research's conceptual framework. With uniform measurement, respondents' responses could be compiled into scores that were subsequently used in descriptive and multivariate analyses. The use of a Likert scale also aligns with common practice in quantitative social research for measuring professional perceptions and attitudes (Babbie, 2021; Bryman, 2022; Hair et al., 2021).

Data Collection Procedures

Primary data was collected through an online questionnaire using Google Forms distributed to the CFEs included in the study's target group. The online format was used to facilitate distribution of the instrument to the professional group while ensuring that responses were obtained in a uniform format. Before completing the questionnaire, respondents received information about the study's purpose and participation requirements. Each respondent then provided informed consent to participate before gaining access to all questions. The use of an

electronic questionnaire also supported respondent anonymity, as neither individual nor organizational identities were used in the analysis. The data obtained were then systematically compiled for subsequent statistical analysis (Babbie, 2021; Bryman, 2022; Hair et al., 2021).

Data Analysis Techniques

Data were analysed using IBM SPSS version 26. The initial stage of analysis was conducted using descriptive statistics to describe the characteristics of respondents and the distribution of each research variable. Next, multiple linear regression was used to examine the effect of AI Readiness, Digital Forensic Competency, and Data Governance Practices on Fraud Detection Effectiveness. This analysis allowed the study to identify the direction, magnitude of influence, and level of significance of each predictor after the influence of other variables in the model was controlled. In addition to individual influences, the overall significance of the model was also examined to determine whether the three independent variables jointly contributed to Fraud Detection Effectiveness. Multiple linear regression was deemed appropriate because the study had one composite dependent variable and three independent variables tested in one statistical model (Field, 2024).

Before interpreting the regression results, the data were examined through a number of assumption tests, including normality, linearity, multicollinearity, independence of errors, and homoscedasticity. Normality was examined using skewness, kurtosis, and residual histogram values. Multicollinearity was evaluated based on tolerance and Variance Inflation Factor (VIF) values, while residual independence was examined using the Durbin–Watson statistic. Homoscedasticity was evaluated through a scatterplot between standardized residuals and standardized predicted values. These steps were carried out so that the relationship between variables could be analysed using a regression model based on data that met the necessary statistical requirements. The test results indicate that the dataset has met the main assumptions of multiple linear regression and can be used in hypothesis testing.

RESULTS AND DISCUSSION

Research Profile and Respondent Characteristics

This study analyses the effectiveness of fraud detection (Fraud Detection Effectiveness) in Certified Fraud Examiners (CFEs) in Zimbabwe affiliated with ACFE Zimbabwe Chapter 128. The focus of the study is directed at three main factors, namely Artificial Intelligence Readiness, Digital Forensic Competency, and Data Governance Practices. These three variables are analysed to determine their individual and simultaneous influence on the effectiveness of fraud detection. The research data was obtained through a structured online questionnaire and a total of 117 complete responses were used in the statistical analysis. This number has exceeded the minimum sample requirement based on the provisions of $N \geq 50 + 8m$, which for three independent variables requires at least 74 respondents. Thus, the amount of data analysed is considered sufficient to support testing using multiple linear regression.

Respondent characteristics indicate that the study involved practitioners with relatively diverse levels of experience and professional backgrounds. Based on gender, 95 respondents, or 81.2%, were male, while 22 respondents, or 18.8%, were female. In terms of age, the largest group was in the 40–49 age range (58 people, or 49.6%), followed by 30-39 age range (33 people or 28.2%), ≥ 50 years constitutes (17 people or 14.5%), and the 20–29 age group (9

people, or 7.7%). This distribution indicates that the majority of respondents were in the professional age group with considerable experience in fraud examination and investigation activities.

Table 1. Demographic Characteristics of Respondents

Characteristics	Category	N	Percentage
Gender	Man	95	81.2%
	Woman	22	18.8%
Age	20–29 years	9	7.7%
	30–39 years	33	28.2%
	40–49 years	58	49.6%
	≥50 years	17	14.5%
Professional experience	<5 years	16	13.7%
	5–10 years	26	22.2%
	11–15 years	22	18.8%
	>15 years	53	45.3%
Employment sector	Public sector	56	47.9%
	Private sector	46	39.3%
	NGO	5	4.3%
	Other	10	8.5%
Education/qualifications	Degree	17	14.5%
	Master's degree	31	26.5%
	Professional certification	66	56.4%
	Doctorate	3	2.6%

In terms of professional experience, most respondents have quite extensive experience. Fifty-three (53) respondents (45.3%) have more than 15 years of experience, while 26 respondents (22.2%) have between 5–10 years of experience, 22 respondents (18.8%) have 11–15 years of experience, and 16 respondents (13.7%) have less than five years of experience. Based on employment sector, 47.9% of respondents work in the public sector and 39.3% in the private sector, while respondents from NGOs and other categories account for 4.3% and 8.5%, respectively. In terms of qualification level, the majority of respondents, 56.4%, hold professional certification. This composition indicates that the data were obtained from respondents who have substantial exposure to auditing, investigations, fraud examinations, and other anti-fraud activities.

Description of Research Variables and Instrument Reliability

The study used four main constructs: AI Readiness, Digital Forensic Competency, Data Governance Practices, and Fraud Detection Effectiveness. Each variable was measured using seven items on a five-level Likert scale. AI Readiness measures the readiness of technological infrastructure, technical skills, training, management support, AI integration, financial capability, and organizational policies in adopting AI. Digital Forensic Competency measures respondents' ability to identify, collect, maintain, analyse, document, and present digital evidence. Data Governance Practices assesses data quality, access control, audit trails, information reliability, data management policies, compliance, and data security. Meanwhile, Fraud Detection Effectiveness describes accuracy, timeliness, investigative efficiency, fraud reduction, evidentiary capabilities, the benefits of detection tools, and successful prosecutions.

Reliability testing showed that all constructs had adequate internal consistency. AI Readiness produced a Cronbach's Alpha value of 0.860, Digital Forensic Competency of 0.918, Data Governance Practices of 0.927, and Fraud Detection Effectiveness of 0.899. All values were above the minimum threshold of 0.70. The overall instrument also obtained a Cronbach's Alpha of 0.834. These findings indicate that the items used in each construct consistently measure the intended concept, so the instrument can be used in further statistical analysis.

Table 2. Reliability **Test Results**

Variables	Number of Items	Cronbach's α	Interpretation
AI Readiness	7	0.860	Good
Digital Forensic Competency	7	0.918	Very good
Data Governance Practices	7	0.927	Very good
Fraud Detection Effectiveness	7	0.899	Good
Overall instrument	4 constructs	0.834	Good

Descriptive Statistics of Research Variables

Based on descriptive statistical analysis, the AI Readiness variable obtained an average value of 2.86 with a standard deviation of 0.882, making it the construct with the lowest average among the four research variables. Digital Forensic Competency had an average of 3.48 with a standard deviation of 0.829, while Data Governance Practices obtained the highest average of 3.61 with a standard deviation of 0.893. Fraud Detection Effectiveness as the dependent variable had an average of 3.53 and a standard deviation of 0.814. The difference in the average values provides an overview of respondents' perceptions of the state of technology, forensic capabilities, information governance, and the effectiveness of fraud detection in their work environment.

Table 3. Descriptive Statistics and Normality of Variables

Variables	Mean	Elementary School	Skewness	Kurtosis
AI Readiness	2.86	0.882	0.374	-0.462
Digital Forensic Competency	3.48	0.829	-0.525	0.014
Data Governance Practices	3.61	0.893	-0.454	-0.255
Fraud Detection Effectiveness	3.53	0.814	-0.551	0.002

Descriptive findings indicate that AI readiness is at a relatively lower level than digital forensic competencies and data governance practices. Conversely, Data Governance Practices produced the highest average score. However, the difference in average scores cannot yet be used to conclude the influence of each variable on fraud detection effectiveness. Therefore, the study continued the analysis by testing regression assumptions and multiple linear regression to determine the contribution of each factor to fraud detection effectiveness.

Regression Assumption Testing

The results of the normality test indicate that the data meets the assumptions of a normal distribution. The skewness values for all variables range from -0.551 to 0.374, while the kurtosis values range from -0.462 to 0.014. These values are supported by the residual histogram, which shows a pattern approaching a bell-shaped distribution. Based on these results, the data are considered sufficiently close to a normal distribution to permit the use of parametric statistical

procedures and linear regression.

The histogram was used as a visual inspection of the residual distribution. The histogram pattern indicates a distribution that relatively resembles a normal curve. These visual results are consistent with the skewness and kurtosis values, so there is no indication of distribution deviation large enough to invalidate the use of multiple linear regression. Thus, the research data meets one of the important requirements before testing the relationship between AI Readiness, Digital Forensic Competency, Data Governance Practices, and Fraud Detection Effectiveness.

Further multicollinearity testing showed that the three independent variables did not experience excessive correlation with each other. AI Readiness had a tolerance value of 0.630 and a VIF of 1.587, Digital Forensic Competency had a tolerance value of 0.718 and a VIF of 1.393, while Data Governance Practices had a tolerance value of 0.565 and a VIF of 1.770. All tolerance values were above 0.10, and the VIF was well below the threshold of 10. Thus, each independent variable still provided different explanatory information regarding Fraud Detection Effectiveness and was worthy of being included simultaneously in the regression model.

Table 4. Multicollinearity Test Results

Predictor	Tolerance	VIF	Condition Index	Conclusion
AI Readiness	0.630	1,587	8.97	There is no multicollinearity
Digital Forensic Competency	0.718	1,393	12.04	There is no multicollinearity
Data Governance Practices	0.565	1,770	12.74	There is no multicollinearity

Furthermore, residual independence was tested using the Durbin–Watson statistic of 2.286. A value relatively close to 2 indicates the absence of significant residual autocorrelation. Homoscedasticity testing was also performed using a scatterplot of standardized residuals against standardized predicted values. The scatterplot showed no systematic pattern, so the residual variance was assessed as relatively constant across various predicted values. Based on this series of tests, the assumptions required in multiple linear regression have generally been met.

Multiple Linear Regression Results

The main analysis of the study was conducted using multiple linear regression to determine the contribution of AI Readiness, Digital Forensic Competency, and Data Governance Practices to Fraud Detection Effectiveness. The model summary results showed an R value of 0.768, R^2 of 0.589, Adjusted R^2 of 0.579, and Standard Error of Estimate of 0.528. The R^2 value of 0.589 indicates that the three independent variables together are able to explain 58.9% of the variation in Fraud Detection Effectiveness, while approximately 41.1% of the other variation is outside the variables included in the research model. After adjusting for the number of predictors, the model is still able to explain 57.9% of the variation in the dependent variable.

Table 5. Summary of Multiple Linear Regression Models

Model	R	R^2	Adjusted R^2	SEE
1	0.768	0.589	0.579	0.528

The ANOVA results indicate that the overall regression model is significant. The F value obtained is 54.073 with a significance level of $p < 0.001$. The regression sum of squares is 45.286, while the residual is 31.546 and the total is 76.832. These results indicate that the use of the three independent variables simultaneously provides a statistically significant model in explaining changes in Fraud Detection Effectiveness among study respondents. Thus, AI readiness, digital forensic competency, and data governance practices, when considered together, have a significant relationship with fraud detection effectiveness.

Table 6. ANOVA Regression Results

Source	SS	df	MS	F	p
Regression	45,286	3	15,095	54,073	<0.001
Residual	31,546	113	0.279		
Total	76,832	116			

The Influence of AI Readiness on Fraud Detection Effectiveness

The results of the first hypothesis test show that AI Readiness has an unstandardized regression coefficient of 0.093, a standardized beta of 0.101, a t-value of 1.330, and a significance value of $p = 0.186$. A positive coefficient indicates a positive relationship, but a significance value greater than 0.05 indicates that the effect is not statistically significant after Digital Forensic Competency and Data Governance Practices are controlled in the model. Thus, the increase in AI Readiness in the research data does not provide sufficient statistical evidence to state that the variable independently increases Fraud Detection Effectiveness. The first hypothesis stating that there is a significant positive effect of AI Readiness on Fraud Detection Effectiveness therefore does not receive empirical support.

The Influence of Digital Forensic Competency on Fraud Detection Effectiveness

In contrast to AI Readiness, Digital Forensic Competency demonstrated a positive and significant effect on Fraud Detection Effectiveness. The unstandardized regression coefficient for this variable was 0.252, the standardized beta was 0.257, the t-value was 3.607, and $p < 0.001$. This means that, with other variables controlled, a one-unit increase in Digital Forensic Competency is associated with a 0.252-unit increase in Fraud Detection Effectiveness. These results demonstrate the importance of professional skills in identifying, collecting, preserving, analysing, documenting, and interpreting digital evidence in the fraud investigation process. Based on these results, the second hypothesis receives empirical support.

The Influence of Data Governance Practices on Fraud Detection Effectiveness

Data Governance Practices is the variable with the largest independent contribution in the research model. This variable has an unstandardized regression coefficient of 0.488, a standardized beta of 0.536, a t-value of 6.681, and $p < 0.001$. Holding other variables constant, a one-unit increase in Data Governance Practices is associated with a 0.488-unit increase in Fraud Detection Effectiveness. The large standardized beta also indicates that its contribution is stronger than Digital Forensic Competency and AI Readiness. These findings illustrate that information quality, data management systems, security mechanisms, access control,

information reliability, and governance structures are important components in supporting the effectiveness of fraud detection among research respondents. The third hypothesis is thus supported by the research data.

Table 7. Multiple Linear Regression Coefficients

Predictor	B / Unstandardized β	Standardized β	t	p	VIF
Constant	0.627	–	2,613	0.010	–
AI Readiness	0.093	0.101	1,330	0.186	1,587
Digital Forensic Competency	0.252	0.257	3,607	<0.001	1,393
Data Governance Practices	0.488	0.536	6,681	<0.001	1,770

Based on these coefficients, the research regression model can be simply written as Fraud Detection Effectiveness = 0.627 + 0.093 (AI Readiness) + 0.252 (Digital Forensic Competency) + 0.488 (Data Governance Practices). This equation indicates that all predictor coefficients are positive. However, statistical significance shows that only Digital Forensic Competency and Data Governance Practices have a significant independent influence in the model, while AI Readiness is not significant at the 5% confidence level. Thus, the presence and readiness of AI alone do not show a strong independent influence when investigator capability and data governance factors are also taken into account.

Simultaneous Effects and Summary of Research Findings

The fourth hypothesis tested the simultaneous influence of AI Readiness, Digital Forensic Competency, and Data Governance Practices on Fraud Detection Effectiveness. The analysis yielded $R^2 = 0.589$, $F = 54.073$, and $p < 0.001$. These results indicate that the three organizational capabilities collectively have a significant influence and can explain more than half of the variation in fraud detection effectiveness in the study sample. Therefore, although AI Readiness is not significant individually, its presence as part of a combination of technology, professional capabilities, and governance remains significant in the overall model. The fourth hypothesis thus receives empirical support.

Overall, the research results provide four main findings. First, the level of AI readiness has a positive but independently insignificant influence on Fraud Detection Effectiveness. Second, Digital Forensic Competency has a positive and significant influence, so that increased professional competence is related to increased ability to detect and prove fraud. Third, Data Governance Practices has the strongest positive influence among the tested predictors. Fourth, the three variables simultaneously explained 58.9% of the variation in Fraud Detection Effectiveness among the 117 Certified Fraud Examiners who participated in the study. These findings illustrate that the effectiveness of fraud detection in the research context is not only a matter of readiness to adopt technology, but also related to human competence and the quality of governance of the information used in investigations.

Table 8. Summary of Hypothesis Testing Results

Hypothesis	The relationship is tested	Statistical results	Decision

H1	AI Readiness → Fraud Detection Effectiveness	β = 0.093; p = 0.186	Not supported
H2	Digital Forensic Competency → Fraud Detection Effectiveness	β = 0.252; p < 0.001	Supported
H3	Data Governance Practices → Fraud Detection Effectiveness	β = 0.488; p < 0.001	Supported
H4	AIR + DFC + DGP → Fraud Detection Effectiveness	R^2 = 0.589; F = 54.073; p < 0.001	Supported

General Meaning of Research Findings on Fraud Detection Problems

This study begins with the issue that the increasing digitization of transactions and the use of technology in financial activities does not automatically make organizations more effective in detecting fraud. The results of the study of 117 Certified Fraud Examiners affiliated with ACFE Zimbabwe Chapter 128 showed that the effectiveness of fraud detection is better understood as the result of a combination of technological readiness, professional competence, and organizational governance. The regression model showed that AI Readiness, Digital Forensic Competency, and Data Governance Practices together were able to explain 58.9% of the variation in Fraud Detection Effectiveness with a value of F = 54.073 and p < 0.001. The large proportion indicates that the three aspects tested are important in explaining why one organization is more effective than another in detecting fraud. However, the influence of each variable is not the same: Data Governance Practices is the factor with the largest contribution, followed by Digital Forensic Competency, while AI Readiness does not show a significant independent effect.

These findings directly address the urgency of previous research, which focused on the changing nature of fraud due to digitalization. Technologies such as artificial intelligence, big data, cloud computing, and advanced analytics provide the ability to process large amounts of data, detect abnormal transactions, and facilitate faster investigations. However, the increasing complexity of technology-enabled fraud means that technology cannot operate independently of investigator capabilities and data control systems. Previous research reviewed in this paper also emphasizes that digital evidence must be managed systematically and meet professional and legal standards. Therefore, the key issue is not simply whether an organization has or is ready to use AI, but rather whether it has professionals capable of interpreting the information and whether the data used is trustworthy, traceable, protected, and accountable.

AI Readiness and Fraud Detection Effectiveness

The results of the study show that AI Readiness has a positive coefficient of β = 0.093, but it is not statistically significant with p = 0.186. Thus, AI readiness has not been proven to have a significant independent influence on Fraud Detection Effectiveness when Digital Forensic Competency and Data Governance Practices are included simultaneously in the model. This finding is important because it shows that infrastructure ownership, organizational support, technology adoption policies, or readiness to use AI do not necessarily directly improve an organization's ability to detect and prove fraud. In other words, there is a difference between readiness to adopt technology and the ability to utilize that technology effectively in real investigative activities.

These findings differ somewhat from previous literature. Previous studies view organizational readiness as a critical condition for successful AI adoption because it can facilitate technological innovation and implementation. Dwivedi et al. (2021) also emphasize the importance of technological infrastructure, management support, facilitating conditions, and regulatory frameworks in achieving the benefits of AI. Based on these previous studies, theoretically, more prepared organizations should have a greater opportunity to utilize AI to improve analytical and decision-making capabilities. However, the results of this study show that this relationship does not automatically occur in the context of Certified Fraud Examiners in Zimbabwe. This is an important contribution of this research because it demonstrates that technological readiness cannot be equated with effective technology use.

One possible explanation for these results is the organizational and technological environment in Zimbabwe. The research paper indicates that there are still limitations in technological infrastructure, resources, advanced digital skills, and AI implementation capacity. In such situations, organizations may have the desire, policy, or initial readiness to adopt AI, but have not been able to translate this into effective operational use. The Unified Theory of Acceptance and Use of Technology (UTAUT) perspective also helps explain this situation, as technology use depends not only on readiness but is also influenced by facilitating conditions, user competence, performance expectancy, effort expectancy, and actual utilization. Therefore, AI Readiness is more appropriately positioned as an enabling condition, rather than the sole determinant of improved fraud detection performance.

The implication is that organizations should not rely solely on the purchase of AI devices, software, or declarations of digital transformation as indicators of success. A more relevant solution is to integrate technology investments with professional training, ongoing technical support, organizational change management, adequate infrastructure, and clear governance. If this approach is adopted, AI can serve as a tool that accelerates data processing, identifies abnormal patterns, and provides analytical information for investigators. Conversely, if AI is implemented without user competence and quality data, its benefits for fraud detection can be limited. This research therefore shifts the focus from simply "having AI" to "building an ecosystem that enables AI to work effectively."

Digital Forensic Competency and Fraud Detection Effectiveness

In contrast to AI Readiness, Digital Forensic Competency was shown to have a positive and significant effect on Fraud Detection Effectiveness with $\beta = 0.252$ and $p < 0.001$. These results indicate that increased digital forensic knowledge, technical skills, and investigative abilities are significantly related to increased fraud examiners' ability to detect, analyse, and investigate fraud. In the context of increasingly digitalized transactions, fraud examiners need more than just an understanding of conventional audits and financial examinations. They also need to be able to identify electronic evidence, collect and preserve data, analyse digital evidence, document results, and present findings in a credible manner.

These findings are consistent with those of Ngai et al. (2011), who demonstrated that advances in digital technology have transformed fraud investigation activities and enabled investigators to analyse large amounts of electronic evidence more efficiently. Murinda and Chiwariro (2023) also demonstrated that organizations with better forensic capabilities are more able to identify anomalies, reconstruct transactions, and uncover fraud patterns that may be

difficult to detect using traditional methods. Meanwhile, Kranacher et al. (2022) emphasize the importance of the ability to acquire, preserve, analyse, and interpret electronic evidence to maintain its integrity and admissibility. Therefore, the results of this study strengthen previous literature and provide additional empirical evidence from Zimbabwe.

From the perspective of the Fraud Pentagon Theory, competency plays a crucial role in understanding the fraud environment. While the theory initially explains the factors that enable fraudsters to carry out their actions, this study uses competency to emphasize the importance of investigators' professional abilities in dealing with increasingly complex frauds. Improving digital forensic capabilities can strengthen an organization's capacity to recognize, track, and respond to fraudulent activities using digital systems. Therefore, digital forensic competency contributes not only to the speed of investigations but also to the quality of evidence, the accuracy of evidence interpretation, and the organization's ability to confront increasingly sophisticated financial crime methods.

A practical solution emerging from these findings is the need for continued investment in human capital. According to ACFE Zimbabwe Chapter 128, organizations employing CFEs, regulators, and professional education providers need to enhance continuous professional development through digital forensic certification, investigation simulations, forensic tool training, and learning about electronic evidence management. By strengthening these competencies, investigators will be better equipped to transform digital system output into credible investigative evidence. The ultimate impact will not only be an increased ability to detect fraud but also an improved quality of evidence and the reliability of investigative results.

Data Governance Practices as a Dominant Factor

The strongest finding in this study comes from Data Governance Practices with a coefficient of $\beta = 0.488$ and $p < 0.001$, making it the predictor with the largest independent contribution to Fraud Detection Effectiveness. This finding indicates that the quality of fraud detection is highly dependent on how an organization manages the data used during the investigation process. Data that is accurate, complete, secure, consistent, accessible with the right authority, and has a clear audit trail provides a stronger foundation for investigators to identify suspicious transactions and build evidence. Conversely, if data is fragmented, inconsistent, difficult to trace, or lacks adequate controls, the capabilities of technology and investigators can be reduced.

The results of this study align with the view that data governance improves information quality, data consistency, accountability, and compliance (COSO, 2022). Rikhardsson and Yigitbasioglu (2018) also demonstrated that effective governance supports an organization's ability to identify suspicious transactions by ensuring fraud detection systems operate using accurate and reliable data. Furthermore, data governance can be viewed not only as an information management activity but also as part of accountability, data security, policy implementation, and strategic decision-making. The consistency between previous research and the current findings strengthens the argument that data governance is a core component of an organization's ability to detect fraud.

The dominance of Data Governance Practices also explains the weak independent influence of AI Readiness. AI and digital forensic systems fundamentally rely on processed data. If the incoming data is incomplete, inaccurate, unintegrated, or difficult to verify, even

sophisticated technology can produce less reliable output. Therefore, technology investment must be preceded by, or at least concurrent with, strengthening data quality. These findings demonstrate that fraud detection issues are not solely about a lack of tools, but also about the quality of the information that is the primary resource for tools and investigators to work with.

From a UTAUT perspective, data governance can be viewed as one of the conditions supporting the effective use of technology. Meanwhile, within the Fraud Pentagon Theory framework, governance mechanisms are related to strengthening controls that can reduce the opportunity for fraud. Strong data governance improves transparency, accountability, data integrity, and organizational oversight, thus not only helping to detect fraud but also strengthening the organization's control structure. Therefore, recommended solutions include establishing formal data governance policies, designating clear data owners, strengthening data-quality management procedures, implementing cyber-security controls, maintaining audit trails, and conducting periodic governance audits.

Simultaneous Influence and Response to Research Urgency

The simultaneous influence of these three variables provides one of the most important answers to the initial research problem. The R^2 value of 0.589 indicates that 58.9% of the variation in Fraud Detection Effectiveness can be explained by AI Readiness, Digital Forensic Competency, and Data Governance Practices together. These results demonstrate that fraud detection cannot be explained by a single organizational capability. Technology provides analytical capability, investigator competence ensures information can be interpreted and used as evidence, while data governance ensures that the information is accurate, secure, complete, and accountable. All three work as complementary resources.

This also explains why a strategy that relies solely on technology acquisition has limitations. AI can enhance the ability to detect abnormal patterns, but investigators are still needed to assess context, verify evidence, and exercise professional judgment. At the same time, even highly competent investigators face limitations when organizational data is incomplete or unreliable. Therefore, effective fraud detection requires an integrated organizational ecosystem that combines technological readiness, human capabilities, and governance. This perspective is consistent with Dwivedi et al. (2021), who emphasize that the value of technology is maximized when supported by skills, facilitating conditions, and other organizational capabilities.

The impact of this integrated approach is the creation of a more robust fraud detection process from upstream to downstream. Data governance ensures the quality of information sources, AI and analytical technology help identify anomalies more quickly, while digital forensic competency ensures findings can be analysed, documented, and developed into investigative evidence. With this approach, organizations not only detect risk signals but also have the ability to provide more credible evidence and follow-up. In the long term, this combination can strengthen fraud risk management and resilience against increasingly complex financial crimes.

Comparison of Findings with Novelty and Research Gap

The novelty of this research stems from the fragmentation of previous research. Studies on AI tend to focus on technological capability and organizational readiness; digital forensic research focuses on investigative competency; while data governance studies often focus on

standalone data quality, accountability, internal control, and evidence management. Limited research simultaneously examines these three variables among Certified Fraud Examiners in Zimbabwe. Therefore, the novelty of this research lies not simply in the use of AI, digital forensics, or data governance variables individually, but in integrating all three into a single empirical model to explain fraud detection effectiveness in a developing country context.

The research results successfully provide evidence supporting this novelty. The findings that Data Governance Practices are the strongest factor, Digital Forensic Competency is significant, but AI Readiness is independently insignificant indicate that the relationship between variables is more complex than the assumption that technology directly improves fraud detection. This research demonstrates that organizational capability is more appropriately understood multidimensionally. This extends UTAUT by showing that technological readiness requires complementary capabilities to produce operational outcomes. At the same time, the research results expand the use of the Fraud Pentagon Theory by placing investigator competence and organizational controls as critical elements in the ability to detect and respond to fraud, not just in understanding how fraud occurs.

Another novel contribution of this research is the contextual evidence from Zimbabwe. Many previous studies have come from broader international contexts or countries with varying levels of technological and institutional readiness. The findings of this study demonstrate that in emerging economies, AI readiness can lose its independent influence when confronted with issues of human competence and governance. Thus, the results of this study do not simply replicate previous findings but provide new insights that technology needs to be positioned as part of a larger organizational system. This research data reinforces the need to view fraud detection as an integrative capability, rather than as a direct consequence of digitalization or AI adoption alone.

CONCLUSION

This study aimed to examine the associations of Artificial Intelligence (AI) Readiness, Digital Forensic Competency, and Data Governance Practices with Fraud Detection Effectiveness among Certified Fraud Examiners (CFEs) affiliated with the Association of Certified Fraud Examiners (ACFE) Zimbabwe Chapter 128. The findings indicated that fraud detection effectiveness was more strongly associated with investigators' professional competencies and the quality of data governance than with technological readiness alone. Digital Forensic Competency demonstrated a positive and statistically significant association with Fraud Detection Effectiveness, while Data Governance Practices emerged as the strongest predictor in the research model. Conversely, AI Readiness exhibited a positive but statistically insignificant association after accounting for the other independent variables. Collectively, the three predictors explained 58.9% of the variance in Fraud Detection Effectiveness, highlighting the importance of integrating technological readiness, professional competencies, and effective data governance practices to strengthen organizational fraud detection capabilities.

FUNDING

The author declares that no financial support was received for the conduct of this research and/or publication of this article.

CONFLICT OF INTEREST

The authors declare that this research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

AUTHOR CONTRIBUTIONS

The authors contributed fully to the formulation of the main ideas, library research, analysis and interpretation of the primary texts of the characters, and drafting the manuscript. All authors have approved the final version of the manuscript.

GENERATIVE AI STATEMENT

The authors declare that generative artificial intelligence (AI) was used in the preparation of this manuscript. The authors acknowledge the use of generative AI to help improve the clarity of the language and improve the grammatical structure of the manuscript. This use was carried out in accordance with applicable ethical guidelines regarding the use and disclosure of generative AI in scientific research. Each author has made a substantial intellectual contribution to this work. The entire contents of this manuscript have been carefully reviewed for accuracy, and the authors are solely responsible for the integrity and final content of this manuscript.

REFERENCES

Ahmed, M., Mahmood, A. N., & Islam, M. R. (2016). A survey of anomaly detection techniques in financial domain. *Future Generation Computer Systems, 55*, 278–288. https://doi.org/10.1016/j.future.2015.01.001

Andaru, F. M., & Utami, B. P. (2024). The convergence of 5.0 and forensic accounting: Leveraging blockchains for effective corruption prevention in Indonesia. *Asia Pacific Fraud Journal, 9*(1). https://doi.org/10.21532/apfjournal.v9i1.338

Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*.

Babbie, E. R. (2021). *The practice of social research* (15th ed.). Cengage Learning.

Bryman, A. (2022). *Social research methods* (6th ed.). Oxford University Press.

Chang, V., Di Stefano, A., Sun, Z., & Fortino, G. (2022). Digital payment fraud detection methods in digital ages and Industry 4.0. *Computers and Electrical Engineering*, *100*, 107734.

Committee of Sponsoring Organizations of the Treadway Commission. (2022). *COSO framework.*

Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.

Creswell, J. W., & Creswell, J. D. (2022). *Research design: Qualitative, quantitative, and mixed methods approaches* (6th ed.). SAGE Publications.

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.

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., . . . Williams, M. D. (2021). Artificial intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management, 57*. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Field, A. (2024). *Discovering statistics using IBM SPSS statistics* (6th ed.). SAGE Publications.

Green, S. B. (1991). How many subjects does it take to do a regression analysis? *Multivariate Behavioral Research, 26*(3), 499–510. https://doi.org/10.1207/s15327906mbr2603_7

Hair, J. F., Page, M., & Brunsveld, N. (2021). *Essentials of business research methods* (5th ed.). Routledge.

Ikhsan, W. M., Ednoer, E. H., Kridantika, W. S., & Firmansyah, A. (2022). Fraud detection automation through data analytics and artificial intelligence. *Riset, 4*(2). https://doi.org/10.37641/riset.v4i2.166

Kranacher, M. J., Riley, R. A., & Wells, J. T. (2022). *Forensic accounting and fraud examination* (3rd ed.). Wiley.

Mabior, M. M., & Wanyama, K. W. (2024). Role of forensic investigations in reduction of financial fraud among commercial banks in South Sudan. *International Journal of Finance and Accounting, 3*(1), 1–14. https://doi.org/10.37284/ijfa.3.1.1845

Mangala, D., & Kumari, P. (2017). Auditors' perceptions of the effectiveness of fraud prevention and detection methods. *Indian Journal of Corporate Governance*. https://doi.org/10.1177/0974686217738683

Mashitoh, H., Daurrohmah, E. W., Inan, D. I., & Firman, A. (2023). The analysis of fraud in perspective of fraud pentagon theory: An empirical study in Indonesia. *JATI: Jurnal Akuntansi Terapan Indonesia, 6*(2), 107–120. https://doi.org/10.18196/jati.v6i2.18765

Murinda, G. T., & Chiwariro, R. (2023). Impact of forensic accounting on fraud detection in Zimbabwe's public sector expenditure cycle. *International Journal for Research in Applied Science and Engineering Technology*. https://doi.org/10.22214/ijraset.2023.57067

Mvunabandi, J. D. (2023). Modelling proactive fraud risk management practices in South Africa's non-governmental organisations. *Journal of Accounting and Finance in Emerging Economies*. https://doi.org/10.26710/jafee.v9i3.2618

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems, 50*(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

Rikhardsson, P., & Yigitbasioglu, O. (2018). Business intelligence & analytics in management accounting research: Status and future focus. *International Journal of Accounting Information Systems, 29*, 37–58. https://doi.org/10.1016/j.accinf.2018.03.001

Siahaan, S., Simanjuntak, A., Simanjuntak, W., Silalahi, M., & Tarigan, D. (2023). Information systems and capabilities auditors investigative to effectiveness implementation audit procedure in proving fraud: Case study of the Regional Inspectorate of Karo Regency. *Jurnal Ilmiah Accusi, 5*(2), 128–145. https://doi.org/10.36985/jia.v5i2.789

Sukardi, S. (2022). Reconstruction of financial crime investigation methods in law enforcement in the era of the Industrial Revolution 4.0. *Unnes Law Journal, 8*(1). https://doi.org/10.15294/ulj.v8i1.53059

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478. https://doi.org/10.2307/30036540

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal, 74*(12), 38–42.

Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q., & Li, J. (2021). Intelligent financial fraud detection practices in post-pandemic era. *The Innovation*, *2*(4).