INKUBIS: Jurnal Ekonomi dan Bisnis
Volume 8, Issue 2, 764-773
e_ISSN: 2775-3913
https://inkubis.polteksci.ac.id/index.php/ink/index
DOI: doi.org/10.59261/inkubis.v8i2.247

The Relationship Between Internal Auditors' Personal Characteristics, Digital Forensic Technology, and the Ability to Identify Fraud Red Flags in Financial Statements

***Audry Leiwakabessy**
Politeknik Negeri Ambon, Indonesia

Ennis Sarenah Kriekhoff
Politeknik Negeri Ambon, Indonesia

***Corresponding author:**
Audry Leiwakabessy, Politeknik Negeri Ambon, Indonesia.
✉audryleiwakabessy@gmail.com

Article Info:

Article history:
Received: April 17, 2026
Revised: May 28, 2026
Accepted: June 01, 2026

Keywords:
Digital Forensics; Fraud; Internal Auditor, Red Flags, Technology

Abstract

Background: Financial statement fraud has become more complex in the information age, exposing internal auditors to various challenges in identifying fraud red flags.
Objective: This research analyzes the effects of personal characteristics and digital forensic technology on internal auditors' ability to detect fraud red flags and examines how these two variables interact with each other.
Methods: This study used a quantitative approach with a cross-sectional survey design. Primary data were collected through structured questionnaires administered to 25 purposively selected internal auditors from public companies listed on the Indonesia Stock Exchange. The data were analyzed using multiple regression and moderation analysis with SPSS version 26.
Results: The multiple regression analysis revealed that internal auditors' personal characteristics significantly predicted fraud detection ability ($\beta = 0.487$, $p = 0.005$), as did digital forensic technology ($\beta = 0.298$, $p = 0.030$). The moderation analysis indicated a significant interaction effect ($\beta = 0.018$, $p = 0.036$, $\Delta R^2 = 6.5\%$), suggesting that the two variables synergistically enhance fraud detection. The combined model explained 62.4% of the variance in red flag identification ($R^2 = 0.624$, $F = 18.267$, $p < 0.001$).
Conclusion: The study concludes that combining strong auditors' personal characteristics with appropriate digital forensic technology produces a synergistic effect that significantly enhances fraud red flag detection ($\Delta R^2 = 6.5\%$). Organizations are recommended to invest concurrently in auditor competency development and digital forensic infrastructure, as the interaction effect demonstrates that dual investment yields outcomes exceeding the sum of individual contributions.

To cite this article: Leiwakabessy, A., & Kriekhoff, E. S. (2026). The relationship between internal auditors' personal characteristics, digital forensic technology, and the ability to identify fraud red flags in financial statements. *INKUBIS: Jurnal Ekonomi dan Bisnis*, 8(2), 764–773. https://doi.org/10.59261/inkubis.v8i2.247

INTRODUCTION

The growing sophistication of financial statement fraud in the age of digitization has changed the risk landscape for businesses worldwide, bringing not only potentially severe economic losses but also the danger of undermining stakeholder trust (Smith, 2018). The ACFE report shows that fraud schemes range from basic asset misappropriation and corruption to more complex forms of financial statement fraud. This phenomenon creates significant challenges for the internal audit function, where identifying red flags or early warning indicators can no longer depend solely on reviewing visible transactions. Modern fraud is often hidden in large datasets and complex transaction processes, requiring auditors to sharpen their detection capabilities to identify subtle signals (Udeh et al., 2024).

The personal characteristics of internal auditors, including professional skepticism,

experience, analytical ability, and integrity, are part of the first line of organizational defense in facing these challenges (Anasta et al., 2024). Highly skeptical auditors do not settle for surface-level explanations, while experience and analytical ability enable them to recognize discrepancies that may not be visible to the naked eye. However, auditors remain human, and the human brain has limited cognitive capacity and professional insight when dealing with big data challenges, which involve not only the sheer volume of available data but also its velocity, including real-time values in high-frequency transactions. Audit limitations that still rely on conventional manual procedures may create gaps that allow fraud attempts to bypass detection (Khairunisa, 2025).

This paradox has led to an urgent need for the adoption of digital forensic technology in internal audit practice. Technologies such as data analytics, artificial intelligence (AI), machine learning, and continuous auditing have the potential to filter, examine, and detect anomalous patterns in financial data more quickly and accurately than human auditors alone (Munawarah, 2024). By leveraging intelligent auditing systems, organizations can uncover fraud risks more effectively. This technology is not only an efficiency tool but also a strategic instrument capable of revealing intricate fraud schemes disguised beneath layers of digitization (Gemilang et al., 2024). This creates a strong assumption that the integration of human cognitive advantages, namely personal characteristics, and computational advantages, namely digital forensic technology, can enhance auditors' ability to identify red flags.

However, the existing academic literature shows a research gap in the interaction between these two components. Previous studies have generally examined human factors and technological factors separately, or they have focused more on external auditors than internal auditors (Kleinman et al., 2020). Indeed, the interaction between internal auditors' personal characteristics and their application of forensic technology is expected to produce different detection dynamics, given the unique position of internal auditors in terms of their continuous awareness of organizational operations and culture (Mawlidy et al., 2024). Furthermore, the limited number of studies that specifically test the moderating or synergistic role of digital forensic technology in the relationship between personal characteristics and fraud detection among internal auditors in Indonesia further underlies the need for this research.

Prior literature has examined human factors, such as professional skepticism, experience, and integrity, and technological factors, such as data analytics and AI, as separate determinants of audit effectiveness (Rusli et al., 2025; Wahidahwati & Asyik, 2022). However, studies integrating their synergistic interaction, particularly among internal auditors in emerging economies such as Indonesia, remain scarce. This represents a significant gap because the unique organizational position of internal auditors, who have continuous access to operational processes and organizational culture, may produce distinct fraud-detection dynamics that are not captured in studies of external auditors (Mawlidy et al., 2024). Furthermore, grounding such interaction in Attribution Theory Wahidahwati (2022) has not been adequately explored in the Indonesian internal audit context, underscoring the need for this research.

To address this gap in the literature, the proposed research adopts an integrative approach. The uniqueness of this research lies in its simultaneous examination of internal auditors' personal characteristics and the use of digital forensic technology, while also explaining how digital forensic technology may moderate, or strengthen, the influence of these characteristics on red flag identification ability. This study offers theoretical contributions by expanding knowledge of fraud-detection mechanisms in the digital age, as well as practical implications for organizations in designing internal audit human resource development strategies and targeted technology investment.

Consistent with these goals, the research questions addressed in this paper are as follows: (1) Do the personal characteristics of internal auditors affect their ability to detect fraud warning signs in financial statements? (2) Does the use of digital forensic technology affect the identification of fraud red flags in financial statements? (3) What is the impact of internal auditors' personal characteristics and digital forensic technology on the ability to detect fraud red flags in financial statements?

The objective of this study is to explore and empirically verify these three questions in order to explain the characteristics of human–technology interaction in internal audit. Theoretically, this research contributes to the development of an audit model that combines behavioral and information technology elements. Practically, the implications of the research

findings are expected to provide guidance for company management and regulators in policy-making related to internal auditor competency development, which should focus not only on technical skills but also on the ability to master forensic technology as an enhancer of professional judgment (Hia et al., 2024). These findings offer practitioners insight into the importance of synergy between professional competence and the modern use of technology in constructing an effective supervisory system that is resilient to financial fraud risks.

METHOD

Research Design

This study was conducted using a quantitative approach with a cross-sectional survey design to analyze the relationship between internal auditors' personal characteristics, digital forensic technology, and the ability to identify fraud red flags in financial statements. This design is appropriate because the research variables are examined and observed at a single point in time, allowing the researcher to obtain relevant information about all variables simultaneously.

Population and Sample

The population of this study consisted of internal auditors from public companies in Indonesia listed on the Indonesia Stock Exchange. The sampling technique used in this study was purposive sampling, with the criteria that internal auditors had more than two years of experience and were involved in the financial statement audit process. The study used a sample size of 25 respondents who were selected based on accessibility and willingness to participate in the research. Although the sample size of 25 is limited and represents a constraint of this exploratory study, it is consistent with purposive sampling for studies targeting restricted professional populations (Wahidahwati & Asyik, 2022). The small sample size limits the generalizability of the findings; therefore, future research should employ larger, multi-company samples.

Data Collection Technique

A structured questionnaire was used as the instrument for collecting primary data through an online survey. The questionnaire consisted of four sections: respondent profile, internal auditors' personal characteristics, the use of digital forensic technology, and the ability to identify fraud red flags. A 5-point Likert scale, ranging from 1 = strongly disagree to 5 = strongly agree, was used to measure each variable. The instrument was pretested on 10 respondents before the main questionnaire was distributed to assess its validity and reliability.

Data Analysis Technique

The data were analyzed using descriptive and inferential statistical techniques with IBM SPSS Statistics version 26 software. Regression analysis was preceded by classical assumption tests, namely the normality test, linearity test, multicollinearity test, and heteroscedasticity test. The data analysis method used was multiple regression to examine the effect of internal auditors' personal characteristics and digital forensic technology on the ability to identify fraud red flags. The interaction between the two independent variables was tested through moderation analysis. A significance level of 0.05 was used.

Validity and Reliability Testing

Instrument validity was assessed using Pearson's product-moment correlation, where items with $r > 0.30$ were considered valid. All 15 items across the three constructs demonstrated r values ranging from 0.412 to 0.791 ($p < 0.05$), confirming satisfactory validity. Reliability was assessed using Cronbach's alpha: Personal Characteristics ($\alpha = 0.847$), Digital Forensic Technology ($\alpha = 0.891$), and Ability to Identify Fraud Red Flags ($\alpha = 0.862$). All values exceeded the 0.70 threshold Rusli (2025), indicating strong internal consistency of the research instruments.

Table 1. Operational Definition of Variables

Variable	Operational Definition	Indicators	Scale
Internal Auditor Personal	Individual attributes of internal auditors that	1. Professional skepticism 2. Audit experience 3. Analytical	Likert 1-5

Characteristics (X1)	influence audit performance	ability 4. Integrity 5. Technical competence	
Digital Forensic Technology (X2)	Use of digital technology for fraud analysis and investigation	1. Data analytics tools 2. Continuous monitoring 3. Artificial intelligence 4. Machine learning 5. Automated testing	Likert 1-5
Ability to Identify Red Flags (Y)	Auditor's ability to recognize fraud warning signals	1. Identification of financial anomalies 2. Detection of unusual patterns 3. Recognition of fraud risk 4. Evaluation of internal control 5. Financial ratio analysis	Likert 1-5

RESULTS AND DISCUSSION

Results

Respondent Characteristics

The subjects of this study were 25 internal auditors from a public company in Indonesia, each with at least two years of audit experience. Based on the respondent profiles, most respondents (60%) had 3–5 years of audit experience, 24% had 6–10 years, and 16% had more than a decade of audit experience. The data indicate that 76% of the respondents held an S1 degree in Accounting, 20% held a master's degree or S2 in Accounting, and 4% were certified as Certified Internal Auditors (CIA).

Descriptive Statistics of Research Variables

The characteristics of the data distribution for each research variable are presented through descriptive statistical analysis as follows:

Table 2. Descriptive Statistics of Research Variables

Variable	Mean	Std. Deviation	Minimum	Maximum
Internal Auditor Personal Characteristics (X1)	18.48	3.84	11	25
- Professional Skepticism	3.68	1.03	2	5
- Audit Experience	3.60	1.29	2	5
- Analytical Ability	3.20	1.22	2	5
- Integrity	4.04	0.93	2	5
- Technical Competence	3.48	1.08	2	5
Digital Forensic Technology (X2)	14.52	4.67	6	25
- Data Analytics Tools	2.72	1.37	1	5
- Continuous Monitoring	3.04	1.54	1	5
- Artificial Intelligence	3.04	1.54	1	5
- Machine Learning	2.68	1.38	1	5
- Automated Testing	3.04	1.21	1	5
Ability to Identify Red Flags (Y)	18.16	3.92	11	25
- Identification of Financial Anomalies	3.72	1.14	2	5
- Detection of Unusual Patterns	3.68	1.11	2	5
- Recognition of Fraud Risk	4.00	1.15	2	5
- Evaluation of Internal Control	3.52	1.26	2	5
- Financial Ratio Analysis	3.64	1.11	2	5

Descriptive analysis of the internal auditors' personal characteristics, red flag identification ability, and digital forensic technology variables indicates that the mean values represent the average scores obtained for each variable. The standard deviations show moderate variability across all variables, suggesting that the data are reasonably distributed.

Classical Assumption Tests

Before conducting the regression analysis, classical assumption tests were performed, yielding the following results. The normality test, using the Kolmogorov–Smirnov test, produced

a significance value of 0.142 ($p > 0.05$), indicating that the data were normally distributed. The linearity test showed an F-linearity value of 12.847 with a significance value of 0.001 ($p < 0.05$), indicating a linear relationship between the independent and dependent variables. The multicollinearity test showed tolerance values greater than 0.10 and variance inflation factor (VIF) values below 10 for all variables, indicating that multicollinearity was not present. The heteroscedasticity test, using the Glejser test, produced significance values greater than 0.05 for all variables, indicating that heteroscedasticity was not present.

Multiple Regression Analysis

Multiple regression analysis was conducted to determine the simultaneous effect of internal auditors' personal characteristics and digital forensic technology on the ability to identify fraud red flags in financial statements.

Table 3. Multiple Regression Analysis Results

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	4.728	2.984		1.585	0.125
Personal Characteristics (X1)	0.487	0.156	0.478	3.124	0.005*
Digital Forensic Technology (X2)	0.298	0.128	0.356	2.328	0.030*

Note: *p < 0.05; **p < 0.01

$R^2 = 0.624$; Adjusted $R^2 = 0.590$; F = 18.267; Sig. F = 0.000

The analysis results reveal that the regression model obtained an R^2 of 0.624, indicating that internal auditors' personal characteristics and digital forensic technology can explain 62.4% of the variance in the ability to identify fraud red flags. The F-value was 18.267 ($p < 0.01$), with a significance level of 0.000, showing that the overall regression model is statistically significant.

Hypothesis Testing

- Hypothesis 1: Effect of Internal Auditor Personal Characteristics

The results of the analysis show that the personal characteristics of internal auditors positively and significantly influence the ability to identify fraud red flags ($\beta = 0.487$, $t = 3.124$, $p = 0.005$). The standardized beta coefficient of 0.478 indicates that a one-unit increase in internal auditors' personal characteristics is associated with a 0.478-unit increase in the ability to identify fraud red flags. This finding suggests that internal auditors with high levels of professional skepticism, audit experience, analytical ability, integrity, and technical competence have a greater ability to detect fraud signals in financial statements.

- Hypothesis 2: Effect of Digital Forensic Technology

The effect of digital forensic technology on the ability to identify fraud red flags was positive and significant ($\beta = 0.298$, $t = 2.328$, $p = 0.030$). A standardized beta coefficient of 0.356 suggests that the use of technology makes a significant contribution to the effectiveness of fraud detection. The study demonstrates that data analytics tools, continuous monitoring, artificial intelligence (AI), machine learning, and automated testing provide considerable technological support for internal auditors in recognizing deviations, anomalies, or abnormal transaction patterns.

- Hypothesis 3: Interaction Analysis (Moderation)

A moderation analysis was performed by including an interaction variable, X1 × X2, in the regression model to test the interaction effect between internal auditors' personal characteristics and digital forensic technology.

Table 4. Moderation Analysis Results

Model	**Unstandardized Coefficients**	**t**	**Sig.**
	B	Std. Error	
(Constant)	2.847	3.524	808
Personal Characteristics (X1)	0.421	0.198	2.127
Digital Forensic Technology (X2)	0.267	0.154	1.734
X1*X2 (Interaction)	0.018	8	2.250

R^2 = 0.689; ΔR^2 = 0.065; F Change = 5.063; Sig. F Change = 0.036

The moderation analysis results indicate that the interaction between internal auditors' personal characteristics and digital forensic technology significantly affects the ability to identify fraud red flags (β = 0.018, t = 2.250, p = 0.036). An increase in R^2 of 0.065 suggests that the interaction effect contributes an additional 6.5% to the explained variation in fraud detection ability.

Discussion

Based on the results of the descriptive and inferential analyses, it is evident that the personal characteristics of internal auditors (X1) are the dominant factor in explaining the variability in the ability to detect fraud red flags (Y). This finding supports the perception that, despite advances in audit tools, human factors remain central to the assurance process, as indicated by a standardized beta coefficient of 0.478 and a significance level of 0.005.

The average score of the personal characteristics variable (18.48) is higher than that of the technology variable, indicating that respondent auditors rely strongly on their internal capacities, such as professional skepticism, experience, and integrity, in performing their duties. This is consistent with the research of Sutawijaya (2020), which found that an effective internal audit structure depends on auditor competence and mindset rather than merely on the availability of documented procedures. Professional skepticism, as one dimension of this variable, functions as an initial cognitive filter. Highly skeptical auditors do not accept management representations at face value without independent confirmation, enabling them to detect anomalies that may indicate fraud.

The audit experience dimension, represented by 60% of respondents with 3–5 years of experience, is also a significant factor alongside skepticism. Experience enables auditors to develop heuristics, or practical rules of judgment, for identifying suspicious transaction patterns. This finding aligns with Wahidahwati (2022), who demonstrated that professional skepticism, ethics, and experience each had a significant and positive influence on fraud detection ability among government auditors, supporting Attribution Theory. Similarly, Rusli (2025) found that skepticism combined with audit technology significantly enhanced fraud detection in Indonesia. Experience enables auditors to develop pattern-recognition heuristics for suspicious transaction signatures, forming a cognitive "memory repository" of prior fraud schemes that allows experienced practitioners to recognize fraud indicators more rapidly than novice auditors (Ramadhany et al., 2025).

Additionally, the elements of integrity and technical ability included in the personal characteristics factor cannot be overlooked. Integrity prevents auditors from succumbing to moral hazard or management pressure to ignore findings. As stated by Musa (2018), the combination of skepticism and integrity creates a psychological barrier that prevents auditors from rationalizing unethical behavior. Therefore, the strong positive effect of personal characteristics on fraud detection ability in this study substantiates Attribution Theory within the audit system, wherein the quality of audit results is a direct outcome or reflection of auditors' internal attributes.

Hypothesis 2 states that digital forensic technology has a significant and positive impact on the accuracy of red flag detection (β = 0.298, p = 0.030); therefore, H2 was accepted. However, the descriptive data provide a more nuanced interpretation. Overall, the digital forensic technology variable recorded a lower mean value (14.52) compared with the other two research variables. This suggests a disconnect between awareness of the importance of technology and the extent of technology utilization in practice.

Although the technology beta coefficient (0.356) indicates a positive effect, its magnitude

remains smaller than that of personal characteristics. This condition reflects the reality in the field, where the use of advanced technologies such as artificial intelligence (AI), machine learning, and data analytics in the audit function of public companies in Indonesia remains uneven and faces various obstacles. These obstacles may include high implementation costs, a steep learning curve, and resistance to changes in work culture.

This finding is in line with the view of Hidayati (2021), who emphasized that accounting and management control systems increasingly rely on forensic disciplines to combat cyber fraud, supported by the need for adaptive organizational infrastructure. Fariah (2023) also argues that auditors who use data analytics tools or continuous monitoring systems can scan very large volumes of data more effectively. Such tools are particularly useful for recognizing quantitative and structured anomaly patterns.

Furthermore, the relatively low average score for the technology variable may indicate limitations in audit capability. Sofa (2024) states that "audit competence based only on accounting knowledge is no longer sufficient in the current technological era; it must also be accompanied by data literacy." If auditors' access to technology is limited to basic technical data processing without utilizing advanced features such as automated testing or predictive modeling, technology will remain an underutilized contributor to fraud detection. Consequently, the positive effect found in this study should be regarded as an initial foundation on which organizations can build more aggressive implementation of digital forensic technology, rather than as evidence that current implementation is already optimal.

The key and novel finding of this study is that auditors' personal characteristics provide a significant moderating or interaction effect in the relationship between digital forensic technology and fraud red flag detection. The interaction coefficient of 0.018, with a t-statistic significance level of 0.036 and an increase in R^2 of 6.5% ($\Delta R^2 = 0.065$), shows that digital forensic technology alone cannot fully determine audit success. Instead, auditors' personal characteristics synergistically strengthen the implementation of digital forensic technology in achieving successful audit outcomes (full-text citation).

This finding challenges the deterministic view that "technology replaces the role of the auditor." Instead, it complements the augmented intelligence paradigm, in which artificial intelligence serves to enhance human cognition. Auditors with strong personal characteristics, such as skepticism, experience, and ethical judgment, are better able to maximize the benefits of digital forensic technology. They can distinguish false positives from genuine fraud indicators, identify system errors, and explore the context behind numbers generated by machine learning systems. For example, data analytics may flag a specific transaction as anomalous because it deviates from the average value. However, an auditor with strong analytical ability and experience will determine whether the deviation reflects manipulation or a reasonable business variation. Without robust personal characteristics, technological outputs may be misinterpreted or disregarded. Conversely, without technological support, even highly competent auditors may be overwhelmed by the volume and complexity of contemporary digital transaction data, thereby increasing sampling risk.

This synergistic effect is consistent with the discussion of Parulian (2024), who emphasized simulation-based learning for red flag recognition. Simulation and technology provide a practical environment that enables auditors to train their intuition and skepticism using real-time data. Arianto (2024) states that anti-fraud literacy among the new generation must combine forensic accounting knowledge with technological understanding. The 6.5% increase in detection capability directly demonstrates that dual investment in human resource development and technology produces greater returns than isolated investment in either area alone.

Theoretically, the findings of this research support the fraud detection model by incorporating interaction variables. Previous studies, including Santoso (2024), often treated internal control and forensic accounting as separate domains. The present finding indicates that the effectiveness of technology can vary significantly depending on the individual or group adopting it. This supports a contingency perspective and suggests that technology adoption in auditing must be understood in relation to human agency and contextual factors. This provides a rationale for developing the Technology-to-Performance Chain (TPC) theory by integrating human agency elements into the internal audit context.

In practical terms, this finding provides a clear signal to both public company management

and regulators. First, the recruitment of internal auditors should not only consider technical accounting skills but should also assess candidates' psychological profiles, particularly skepticism and integrity. Second, digital forensic technology training should be specifically tailored to the unique tasks of auditors. Training should improve auditors' technological fluency so that they become confident and willing to use advanced technologies. Third, organizations must create stronger links between technology systems and auditor performance appraisal. For example, organizations may provide incentives to auditors who successfully identify fraud based on digital analysis.

Ultimately, this research proves that combating financial statement fraud in the modern digital era requires a human-and-technology approach, rather than a technology-only approach. Digital forensic technology extends auditors' reach and accuracy, while personal characteristics provide direction, judgment, and ethical intent. The synergy between these two elements, as shown by the significant interaction effect, is essential for building organizational resilience against increasingly complex fraud risks.

CONCLUSION

The findings of this study indicate that the personal characteristics of internal auditors and the use of digital forensic technology have a significant influence on the ability to identify fraud red flags in financial statements. The strong positive effect of internal auditors' personal characteristics on fraud detection ability ($\beta = 0.487$, $p = 0.005$) demonstrates that professional skepticism, audit experience, analytical ability, integrity, and technical competence collectively constitute the most influential determinants of fraud detection capability. Digital forensic technology also yielded a moderate yet significant effect ($\beta = 0.298$, $p = 0.030$), encompassing data analytics tools, continuous monitoring, artificial intelligence and machine learning, and automated testing. Crucially, the interaction between strong personal characteristics and the optimal use of digital forensic technology ($\beta = 0.018$, $p = 0.036$) produced an additional incremental improvement in detection ability. The overall model explains 62.4% of the variance in fraud red flag identification, confirming that an integrative approach combining auditors' personal qualities with advanced technological tools represents the most effective strategy for enhancing fraud detection in internal audit practice.

The theoretical contribution of this study lies in extending Attribution Theory to the internal audit context by demonstrating that individual characteristics, as internal factors, and digital forensic technology, as an enabling external factor, jointly determine fraud detection outcomes. This finding supports the development of a Technology-to-Performance Chain (TPC) model moderated by human agency. Practically, public company management should invest simultaneously in auditor competency development and forensic technology infrastructure, as both elements are mutually reinforcing. Regulators are likewise encouraged to mandate digital forensic technology competency standards within internal auditor certification requirements. Nevertheless, this study has several limitations, including a small purposive sample ($n = 25$) drawn exclusively from publicly listed Indonesian companies, which restricts statistical power and generalizability. The cross-sectional design precludes causal inference, and self-reported Likert-scale data may introduce response bias. Future research should therefore employ larger, multi-industry, and multi-country samples; adopt longitudinal or experimental designs; and incorporate objective fraud detection performance metrics to further validate and extend these findings.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to Politeknik Negeri Ambon, Indonesia, for the institutional support provided throughout this research. We also thank all internal auditors from the public companies listed on the Indonesia Stock Exchange who willingly participated as respondents in this study. Their time and cooperation made this research possible.

AUTHOR CONTRIBUTION STATEMENT

Audry Leiwakabessy contributed to the conceptualization, methodology design, data collection, data analysis, and writing of the original draft. Ennis Sarenah Kriekhoff contributed to the supervision and validation of the manuscript. Both authors are affiliated with Politeknik

Negeri Ambon, Indonesia, and have read and agreed to the published version of the manuscript.

REFERENCES

Anasta, L., Christine, C., Permatasari, P. S., Aulia, S., Ristyanti, A., Nulhakim, F. A., Fadlirahman, M., Fauzia, N. R., & Alkotdriyah, P. P. (2024). *Audit Internal: Teori, Konsep, dan Praktik*. Penerbit Salemba.

Arianto, B. (2024). Pengenalan Akuntansi Forensik dan Literasi Anti Fraud bagi Generasi Z Kota Serang. *Rahmatan Lil'Alamin Journal of Community Services*, 67–78. https://doi.org/10.20885/RLA.Vol4.iss2art2

Fariah, A. (2023). Mengeksplorasi Masa Depan Audit: Memanfaatkan Teknologi dan Analisis Data untuk Peningkatan Integritas Keuangan. *Cakrawala Repositori IMWI*, *6*(4), 1388–1399. https://doi.org/10.52851/cakrawala.v6i4.380

Gemilang, G., Ismaidar, I., & Zarzani, T. R. (2024). Pertanggungjawaban pidana korporasi dalam tindak pidana pencucian uang. *Innovative: Journal Of Social Science Research*, *4*(2), 8455–8471. https://doi.org/10.31004/innovative.v4i2.10027

Hia, W. V., Miharja, K., Damayanti, N., & Angelina, F. J. (2024). Peran Auditor Internal Dalam Meningkatkan Efektifitas Tata Kelola Perusahaan: Studi Kasus Sektor Kesehatan. *Trilogi Accounting & Business Research*, *5*(1), 48–60. https://doi.org/10.31326/tabr.v5i1.2050

Hidayati, A. N., Riadi, I., Ramadhani, E., & Al Amany, S. U. (2021). Development of conceptual framework for cyber fraud investigation. *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, *7*(2), 125–135.

Khairunisa, N. (2025). *Analisis Faktor Pendorong dan Hambatan Adopsi Teknologi Blockchain dalam Mencegah Kecurangan Akuntansi dan Keuangan*. Universitas Islam Indonesia.

Kleinman, G., Strickland, P., & Anandarajan, A. (2020). Why do auditors fail to identify fraud? An exploration. *Journal of Forensic and Investigative Accounting*, *12*(2), 334–351.

Mawlidy, E. R., Dio, R., & Lorensa, L. (2024). Kemampuan artificial intelligence terhadap pendeteksian fraud: Studi literatur. *Akurasi: Jurnal Studi Akuntansi Dan Keuangan*, *7*(1), 89–104. https://doi.org/10.29303/akurasi.v7i1.488

Munawarah, I. (2024). Pengaruh kecerdasan buatan untuk audit keuangan: Meningkatkan efisiensi dan menghadapi tantangan di era digital. *Jurnal GICI Jurnal Keuangan Dan Bisnis*, *16*(2), 125–135.

Musa, K., Saad, N., & Nor, M. A. M. (2018). Tingkah Laku Integriti Dalam Pemantapan Pengurusan Sektor Perkhidmatan Awam: Integrity Behavioral in Order to StrengtheningThe Management of Public Sector Service. *Management Research Journal*, *7*, 260–277.

Parulian, P., Bebasari, N., & Fatmawati, E. (2024). Pelatihan Internal Control untuk Meminimalkan Risiko Fraud dalam Organisasi. *Dedikasi: Jurnal Pengabdian Lentera*, *1*(10), 341–352. https://doi.org/10.59422/djpl.v1i10.1029

Ramadhany, A. A., Erlina, E., Sadalia, I., & Fachrudin, K. A. (2025). Enhancing Fraud Detection Performance: The Interplay of Red Flag Awareness, Self-Efficacy, and Professional Skepticism. *Journal of Risk and Financial Management*, *18*(6), 301. https://doi.org/10.3390/jrfm18060301

Rusli, A. A., Yusnaini, Y., & Sukanto, S. (2025). Enhancing Fraud Detection: Roles of Skepticism, Audit Technology, and Industry Specialization in Indonesia. *Economics, Business, Accounting & Society Review*, *4*(1), 138–150. https://doi.org/10.55980/ebasr.v4i1.203

Santoso, A. H., Aristo, A. R. B., Christianto, E., Andam, S. K., Wijaya, W., Wijaya, H. A., Lituhayu, S., Wibowo, L. E. S., & Aditama, A. K. P. (2024). *Mengungkap jejak: Praktik dan metodologi akuntansi forensik*. SIEGA Publisher.

Smith, S. S. (2018). Digitization and financial reporting–how technology innovation may drive the shift toward continuous accounting. *Accounting and Finance Research*, *7*(3), 240–250.

Sofa, D. M. (2024). Transformasi Digital Akuntansi dalam Perspektif Pendidikan: Eksplorasi Kompetensi dan Kesiapan Kerja Mahasiswa Akuntansi. *JURASIMA*, *2*(2), 15–19. https://doi.org/10.33478/jurasima.v2i2.65

Sutawijaya, I. N., SE, M. A., & Ardeno Kurniawan, S. E. (2020). *Audit Kinerja: Mendorong Peningkatan Value Organisasi Pemerintah dalam Mewujudkan World Class Government*. Penerbit Andi.

Udeh, E. O., Amajuoyi, P., Adeusi, K. B., & Scott, A. O. (2024). The role of big data in detecting and

preventing financial fraud in digital transactions. *World Journal of Advanced Research and Reviews*, *22*(2), 1746–1760.

Wahidahwati, W., & Asyik, N. F. (2022). Determinants of auditors ability in fraud detection. *Cogent Business & Management*, *9*(1), 2130165. https://doi.org/10.1080/23311975.2022.2130165