International Research Journal of Multidisciplinary Scope (IRJMS), 2025; 6(1): 22-36 IRJMS

Original Article | ISSN (O): 2582-631X DOI: 10.47857/irjms.2025.v06i01.02164

Optimizing Internal Audit Practices for Combatting Occupational Fraud: A Study of Data Analytic Tool Integration in Zimbabwean Listed Companies

Himanshu Thakkar*, Gudoshava Chrispen Fanuel, Saptarshi Datta, Priyam Bhadra, Siddharth Baburao Dabhade

School of Management Studies, National Forensic Sciences University, Gandhinagar, Gujarat, India. *Corresponding Author's Email: himanshudthakkar@gmail.com

Abstract

Various types of fraud exist in almost every country, classified as corruption, asset misappropriation, and financial statement fraud. Occupational fraud, a mixture of corruption and asset misappropriation, has been mostly committed within companies, significantly impacting their economic stability. Interview and questionnaire techniques were employed to collect data from the companies listed on the Zimbabwe stock exchange. Primary data has been collected from 44 respondents through questionnaires. It is found that companies in Zimbabwe are widely using Excel for internal audits. Internal audits play a crucial role in fraud prevention and detection, but there is room for improvement, particularly in leveraging data analytics to enhance effectiveness. To prevent occupational fraud, companies in Zimbabwe should strengthen their internal audit mechanism and leverage data analytics tools such as ACL, IDEA, SQL, Power BI, Tableau, Python, and R. These measures can help detect and prevent fraud at an early stage, safeguarding organizational assets and improving the quality of internal audits. In addition to adopting data analytics tools, companies should focus on integrating advanced fraud detection methodologies, such as machine learning and predictive analytics, into their internal audit systems. Regular auditor training on emerging fraud schemes and digital threats is essential for maintaining effective fraud prevention. Establishing stronger internal controls, periodic audits, and fostering a culture of accountability and transparency within organizations can further mitigate the risk of occupational fraud. Furthermore, collaboration with external auditors can provide an independent assessment, adding extra protection against fraud.

Keywords: Asset misappropriation, Data Analytics, Internal Audit, Occupational Fraud.

Introduction

Financial crises and instability have increased fraud scandals, making internal auditing procedures important for companies (1). The rise in financial crises and instability has led to a surge in fraud scandals, underscoring the critical significance of internal auditing procedures for companies. The internal auditors' functions hold great importance in modern businesses as they contribute to attaining an organization's objectives by employing a systematic and disciplined approach to assess and enhance risk management, control, and governance processes (2). The effectiveness of internal auditing can be improved through factors such as the quality of the internal audit function, the competence of the internal audit, the independence of the internal audit function, and management support. Occupational fraud is the most prevalent and significant threat among the various types of fraud that business organizations can encounter (3). Occupational fraud involves deliberate actions carried out within a professional role or occupation. It represents a willful attack on the organization, characterized by intentional deception or concealment to gain personal advantages such as acquiring money, property, or services. Occupational fraud encompasses corruption schemes, asset misappropriation schemes, and financial statement fraud schemes, posing a substantial menace to many organizations that may struggle to protect themselves effectively. The study aims to understand the current use of fraud data analytics tools by the internal auditors in the Zimbabwean listed companies. Further, it also evaluates the challenges faced by internal auditors while using fraud data analytics tools.

(Received 26th August 2024; Accepted 13th January 2025; Published 19th January 2025)

Theoretical Framework and Related Literature

Background

The world has been faced with ever-increasing fraud cases, most perpetrated by the organization's employees. The leading cases are WorldCom, Enron, Satyam, and Tyco fraud cases, and the executives were involved in manipulating the organization's fraud cases. WorldCom capitalized expenses by recording them as investments, and this raised profits to US$3.8 billion in 2001 and by the first quarter of 2002 to US$797 billion (4). In the study done by ACFE report to the nation in 2022, the cases by region revealed that the United States and Canada were leading in the number of cases with a total of 675 reported cases, and the second was sub–Saharan Africa, 429 cases. In its report to the nation, the 2022 Association of Certified Fraud Examiners (ACFE) stated that Zimbabwe was ranked among the top 10 African countries with the highest rates of occupational fraud. The report highlighted that most occupational frauds were committed through asset misappropriation, contributing to 86% of the reported cases. Chitema Brian's article in The Sunday News, dated March 8, 2022, stated that officials at the National Oil Company of Zimbabwe could not account for US$14.6 million (5). A typical example of the demise of an organization was PSMAS, which was affected by corruption and misuse of resources, leading to the closure of some clinics and the failure to provide and pay for services (6). In another case, a report was published by Muzavazi Shakespeare in the ZW News highlighting that an executive member of National Railways of Zimbabwe was fingered in 300 (7). In September 2024, two well-known businessmen committed fraud worth US$1.4 million. In this fraud, the perpetrator has committed occupational fraud. They have submitted fake tax documents to the Zimbabwe Revenue Authority (ZIMRA). This fraud can be identified with the help of fraud data analytics (8). Due to technological advancement, organization's operations have shifted from manual to computerization. The operations have become complex, and the received data volume has grown and requires specialized tools and human resources. The objectives of analytical tools are obtaining necessary and valuable information from collected data and utilizing them for active control and decision-making (9). The rise in technology data sources expanded beyond the traditional database; data sources include emails, mobile device outputs, and sensor-generated data, giving birth to big data (10). The auditing profession has a growing volume of available data that is increasing in variety and veracity (11). Due to the development of IT systems processes, data has grown exponentially, making it difficult for internal control staff to manually look at every transaction, creating the need to use data analysis tools and programs (12). Numerous studies have highlighted the pivotal role played by internal auditors in preventing and detecting fraud. By conducting thorough fraud risk assessments and providing comprehensive fraud awareness training, internal auditors can significantly reduce the occurrence and duration of fraud within organizations. A study on the role of technology in evidence gathering for cases of fraud, focusing on the Bulawayo Central Business District, Zimbabwe, recommended that staff should be trained on the use of technological tools and methods for detecting fraud-related activities (13). The study objective is to look at the effectiveness of internal audits in preventing and detecting occupational fraud using data analytic tools for listed companies in Zimbabwe, as there is limited empirical study evidence on the types of data analytic tools used in the internal audit process. While there is a general understanding that data analytic tools can be effective in detecting fraud, there is a need for research that examines the level of adoption of data analytic tools and the types of occupational fraud that can be detected using these tools.

Literature Review on Occupational Fraud

Fraud is a generic term encompassing all the various means human ingenuity can devise. These means are resorted to by one individual to gain an advantage over another through false representations. No definite and invariable rule can be laid down as a general proposition in defining fraud, as it includes surprise, trickery, cunning, and unfair ways by which another is cheated (14). The only boundaries defining it are those that limit human knavery. Forensic data analytics is essential for spotting early indicators of tax evasion, thereby aiding in fraud prevention (15). The only boundaries defining it are those that limit human knavery. Fraud is a deception that includes the following elements: a representation of a material

point, which is false, and intentionally or recklessly so, which is believed and acted upon by the victim to the victim's damage. Empirical findings from the general banking sector highlight internal auditors' crucial role in preventing and detecting fraud (16). Occupational Fraud is using one's occupation for personal enrichment through deliberate misapplication of the employing organization's resources or assets. The classification of occupational fraud was provided, and three types were identified: corruption, asset misappropriation, and financial statement fraud. Asset misappropriation involves stealing an asset of a company for personal use at the company's expense or misuse of a company's resources. False or misleading records or documents often accompany asset misappropriation to conceal the theft (17). Donald Cressey's fraud triangle highlighted the motivation that drives people to breach their fiduciary duty, identifying three primary factors: pressure, opportunity, and rationalization. Understanding these three factors can help organizations implement measures to prevent and detect fraud when it occurs (18). According to ISA 240, the two types of fraud those are relevant for audit purposes are those that involve intentional fraudulent reporting and those that affect the misappropriation of company assets (19). Asset misappropriation fraud can be categorized into two main types: cash theft and non-cash assets. These fraudulent activities can occur in various situations: (i) before the assets are recorded in the organization's book(s), known as skimming; (ii) while the assets are in the organization's possession (such as theft or misuse of equipment, inventory, supplies or cash), or (iii) during the purchasing process (involving billing, expense reimbursement or payroll schemes). In the last scenario, the organization might end up paying for goods or services that it should not have or may pay an excessive amount for the purchased items or services. Financial statement fraud is the intentional mistake or omission of amounts or disclosures in financial statements to deceive the users of those statements (20). Examples of financial statement fraud include improper revenue recognition, overstatement of inventory, improper deferral liabilities, cookie jar accounting, and inadequate disclosure in footnotes.

Theoretical Framework

Resource-Based View Theory

This research leverages the Resource-Based View (RBV) theory by integrating empowerment strategies to improve the effectiveness of internal auditing. According to RBV theory, organizations are unique due to their distinct capabilities and resources. Empowerments are valuable resources that enable internal auditors to perform their responsibilities more efficiently (21). The Resource-Based View (RBV) theory proposes that organizations are unique because they possess different resources and capabilities. This distinctiveness grants a competitive edge. The theory underscores that possessing valuable, rare, and difficult-to-imitate resources empowers organizations to outperform their rivals and achieve long-term success.

Agency Theory

Within the agency theory framework, an organization is viewed as a network of contracts between executives (agents) who control economic resources and shareholders (principals). A central challenge this framework highlights is the information disparity, as agents generally have greater access to information than principals. This imbalance makes it difficult for the owners to accurately assess whether the managers act in a way that most benefits them (22). This gap makes it difficult for the owners to monitor the managers' actions and ensure they align with their goals.

Stakeholder Theory

Stakeholder theory argues that a company should broaden its focus and consider the well-being and needs of all entities associated with the organization, not just its shareholders. Stakeholders encompass anyone who can be impacted by or has the potential to affect the company's actions (23). This includes employees, customers, suppliers, local communities, and investors. The theory emphasizes that striking a balance between the needs of these various groups is essential for the company's long-term prosperity and sustainability (24). Stakeholder theory emerged as a new framework to address three interconnected business challenges: understanding how value is created and exchanged, connecting ethical considerations with capitalism, and guiding managers towards an approach that resolves the first two issues (25).

Internal Audit

Current internal auditing (IA) research hasn't significantly improved our understanding of how the internal audit function (IAF) operates. As a result, there is limited knowledge about the factors that make IA practices effective and measurable. Most IA research is dominated by US-based authors and journals, primarily focusing on the American context, mainly publicly listed companies. This research typically relies on positivist analyses and often does not explicitly reference theoretical frameworks. There is a noticeable lack of studies addressing central regions, such as emerging economies, and critical organizational settings, including private small and medium-sized enterprises (SMEs) and not-for-profit organizations (26).

Occupational Fraud

Occupational fraud is likely the most significant threat facing organizations. Consequently, senior management consistently takes steps to safeguard their business operations and collaborations, mainly working closely with internal audit personnel. Internal auditors, encouraged to gain extensive knowledge about fraud, are strategically established and positioned to deliver valuable services to the organization (27). The findings of this study offer useful insights for researchers and business managers, helping to improve their understanding of the factors that predict occupational fraud losses. Specifically, these insights can assist in refining efforts to prevent, detect, and address fraud promptly, thereby reducing the occurrence and impact of such losses (28).

Forensic Data Analytics

An effective way to strengthen the collaboration between forensic scientists and police investigators is by utilizing an Intelligence Analyst (IA) within the forensic services team. The IA acts as a bridge, linking the scientific and law enforcement roles by receiving data post-analysis and converting it into actionable intelligence. This intermediary role marks a paradigm shift, highlighting the growing importance of forensic analysis in investigations. Forensic intelligence involves integrating forensic data early in the investigation and adopting a comprehensive case approach that includes various potential datasets and relevant information (29). The IP reputation system is one effective method for profiling the behaviour of security threats to cyber-physical systems. However, current reputation systems grapple with difficulties such as high management costs, high false-positive rates, long processing times, and reliance on limited data sources for determining IP address reputation. To address these problems, we propose a novel hybrid approach that integrates Dynamic Malware Analysis, Cyber Threat Intelligence, Machine Learning (ML), and Data Forensics. Our approach predicts IP reputation in its pre-acceptance stage by utilising large-scale data forensics. It categorizes associated zero-day attacks through behavioural analysis using the Decision Tree (DT) technique.

Fraud Hexagon

Amid the pandemic, numerous businesses in Indonesia have faced challenges, driving some to manipulate their financial statements to depict a more upbeat performance. This practice, financial statement fraud, is critical to anticipate and prevent. Therefore, it is essential to investigate the factors that drive companies to engage in such fraudulent activities. This study focuses on analysing the fraud hexagon theory and its connection to instances of financial statement fraud (30). This study seeks to identify cases of fraudulent financial reporting by employing hexagon fraud analysis, which encompasses seven key factors: financial stability, external pressures, inadequate monitoring, auditor changes, changes in leadership, arrogance, and conspiracy. The research analyses consolidated audit reports of state-owned enterprises, aiming to explore the factors contributing to fraudulent financial reporting. The motivation for this research stems from contradictory findings in prior studies, the prevalence of fraudulent financial reporting, and the limited application of the hexagon of fraud theory in existing research (31). Data analytics is beneficial for the detection of fraud at early stages. We summarize the conceptual framework in Figure 1 and elaborate on it in the following.

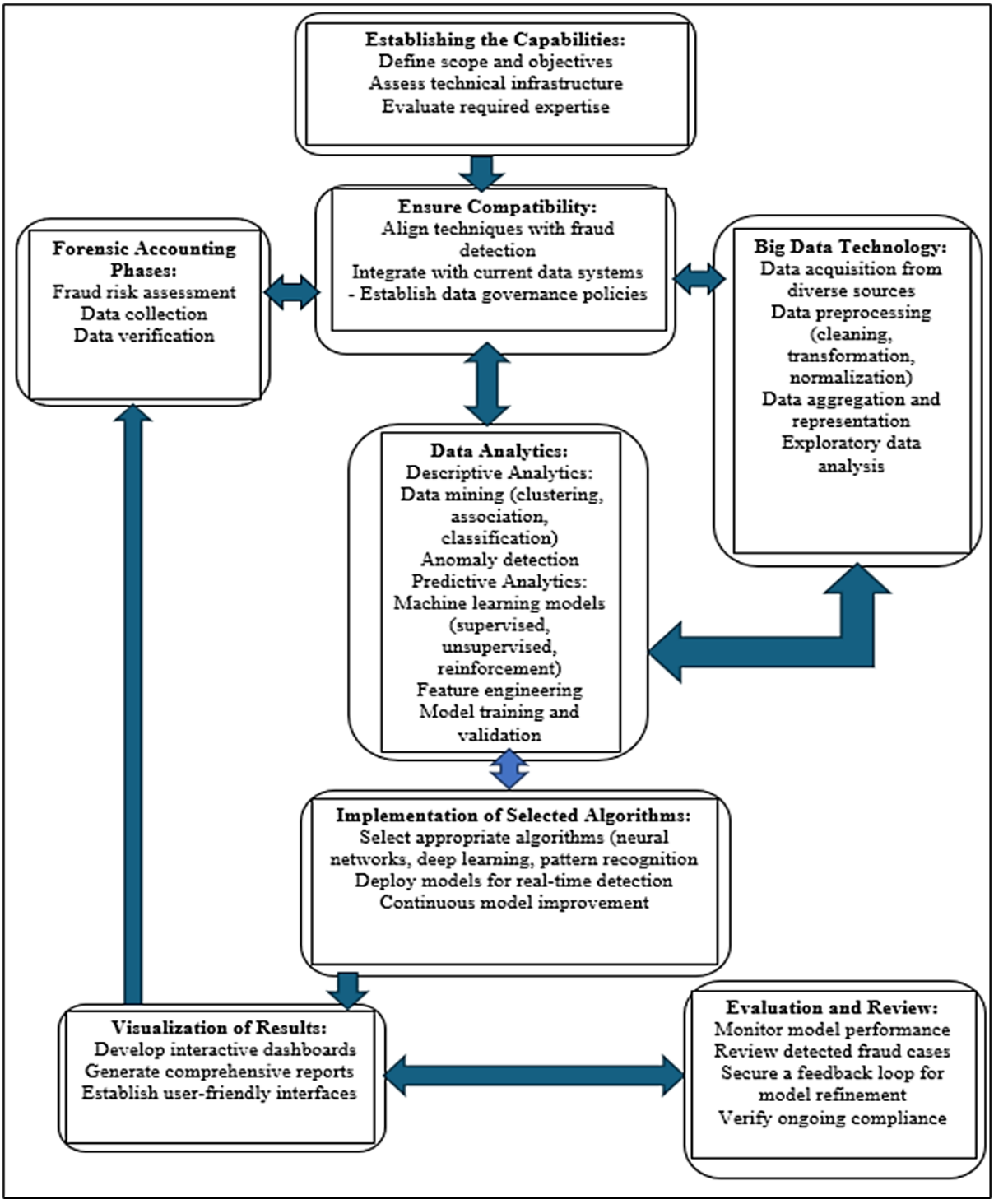

Figure 1: Conceptual Framework for the use of Data Analytics in the Detection of Fraud

This proposed framework shows the critical stages involved in utilizing forensic data analytics to identify occupational fraud in its early stages,

Establish the Capabilities

Scope Definition: Clearly define the scope and objectives of forensic data analytics in the context of early-stage occupational fraud.

Technical Assessment: Evaluate the existing technical infrastructure for data storage, processing, and analytics capabilities. Identify any necessary enhancements or upgrades.

Skill Set Assessment: Assess the expertise required within the organization. This includes data analytics skills, forensic accounting knowledge, and experience with fraud detection techniques.

Ensure Compatibility

Technique Alignment: Align specific forensic data analytics methods to the requirements of

occupational fraud detection. Different techniques may be appropriate for uncovering different types of fraud schemes.

System Integration: Ensure compatibility between the data analytics tools and existing data systems (ERP software, financial systems), adhering to compliance standards.

Data Governance: Implement policies to uphold data integrity, confidentiality, and security throughout the process. This encompasses defining data access controls, data preservation policies, and data anonymization procedures (where applicable).

Data Collection and Preprocessing

Forensic Accounting Phases

Fraud Risk Assessment: Pinpoint areas within the organization most vulnerable to occupational fraud based on industry trends, internal control mechanisms, and historical data.

Data Collection: Collect relevant financial and non-financial data points based on the identified risk areas. This may include transactional data, employee records, communications (emails), and external data sources (public databases).

Data Verification: Verify collected data's trustworthiness, accuracy, and comprehensiveness through verification procedures.

Big Data Technology Phases:

Data Acquisition: Gather data from various sources, including financial systems, CRM, HR databases, emails, and external data sources (with proper authorization).

Data Preprocessing: Perform data cleaning (handling missing values and inconsistencies), data transformation (e.g., formatting dates), and data normalisation to prepare data for analysis.

Data Aggregation: Aggregate data into a unified format suitable for comprehensive analysis.

Exploratory Data Analysis (EDA): Conduct initial data exploration to understand basic patterns and trends and identify potential anomalies.

Data Analytics

Descriptive Analytics: Data Mining: Utilize techniques like clustering, association rule learning, and classification to identify patterns and anomalies in the data that may indicate potential fraud.

Anomaly Detection: Detect irregularities in data that deviate from established patterns or baselines, potentially signifying fraudulent activity.

Predictive Analytics: Machine Learning Models: Implement supervised, unsupervised, and reinforcement learning models to forecast the probability of early-stage occupational fraud.

Feature Engineering: Develop and select features from the data that significantly impact fraud detection accuracy.

Model Training and Validation: Train the models on historical data containing known fraud cases and validate their performance on a separate test dataset.

Implementation of Selected Algorithms

Algorithm Selection: Select appropriate algorithms based on the intricacy of data, varieties of fraud schemes, and intended results. This may involve neural networks, deep learning techniques, or pattern recognition algorithms.

Model Deployment: Deploy the selected models into the production environment for real-time fraud detection and anomaly flagging.

Continuous Improvement: Regularly update and refine models based on new data, evolving fraud patterns, and feedback from fraud investigations.

Visualization of Results

Dashboard Creation: Develop interactive dashboards to visualise data insights, fraud detection results, and key performance indicators (KPIs).

Reporting: Generate comprehensive reports highlighting detected anomalies, potential fraud cases, and supporting data for further investigation.

User-Friendly Interfaces: Ensure user-friendly visualisation tools are accessible to relevant stakeholders (e.g., forensic accountants and internal auditors).

Evaluation and Review

Performance Monitoring: Continuously monitor the performance of deployed models and analytics processes to identify potential improvements in accuracy and efficiency.

Fraud Case Review: Regularly review detected fraud cases to assess the system's effectiveness and refine models for better detection accuracy.

Feedback Loop: Establish a feedback loop incorporating learnings from investigated and confirmed fraud cases into the model refinement process.

Compliance Check: Ensure ongoing compliance with relevant data privacy regulations (e.g., GDPR, CCPA) and industry standards.

Methodology

Research Methodology

The researcher used a mixed research method. The researcher combined quantitative and qualitative methods to provide a complete and robust understanding of the problems and questions rather than selecting either of the designs. The study was based on Research Data collected through the distribution of questionnaires and interviews with internal auditors of Zimbabwe companies. The researcher selected internal auditors due to their expertise in fraud risk management, which involves evaluating the effectiveness and efficiency of internal controls and fraud risks through their involvement in fraud risk management programs. The sample frame used was the Listed Zimbabwe Stock Exchange companies. The study has been conducted on 61 listed Zimbabwe Stock Exchange listed companies. A total of 55 internal auditors were selected as the sample from the 61 targeted respondents across all the listed companies. The popular Slovin formulae were used to determine the sample size from the target population of 61, which is as follows:

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

The formula mentioned above uses symbols to represent different variables. The letter 'n' represents the sample size that needs to be determined, while 'N' represents the target population. The value of 'e' is the standard error, which depends on the researcher's confidence level. In this study, the researcher used a 95 percent confidence level. The target population consisted of 61 internal auditors, 'N' was 61, and the standard error or margin of error was 5 percent, that is, 'e=0.05. Applying the formulae, the results obtained were as follows:

$$n = N/ (1 + Ne^2)$$
$$n = 61/ (1 + 61(0.05^2)$$
$$n= 55$$

After applying the formula, the sample size was found to be 55 respondents, which would be appropriate for this study.

Data Collection

To explore the correlation between variables, this study employed structured questionnaires and unstructured questions for the interview to gather data from internal auditors. The questionnaire consisted of questions designed to be answered on the 5- Likert scale (Strongly Agree (5), Agree (4), Neutral (3), Disagree (2), Strongly Disagree (1)), enabling the collection of quantitative research data that has been analyzed using Microsoft Excel. Descriptive statistics, including mean scores, were used for data analysis.

Prevention and Detection

Preventive controls refer to the manual or automated procedures that prevent undesirable events. On the other hand, detective controls can also be manual or automated, but they aim to uncover an incident that has already occurred. An effective anti-fraud system can considerably minimize an organization's susceptibility to fraud by having an optimal combination of preventive and detective controls (32). The management of an organization has the primary responsibility for preventing and detecting fraud under the oversight of those charged with the governance. The five methods of preventing fraud opportunities are (a). Reasonable internal control, (b). Discouraging collusion between employees and customers or vendors, monitoring employees and creating a whistle-blowing system; (c). Creating expected punishment, and (d). Conducting proactive auditing. Data-driven fraud detection takes a proactive approach; investigators brainstorm potential fraudulent schemes and symptoms and use advanced data analysis techniques to identify and detect such patterns. By being proactive, investigators can stay ahead of possible fraud, mitigate risks, and prevent financial losses more effectively. The proactive (data-driven) method of fraud detection is broken down into six steps: 1. Understand the business, 2. Identify possible frauds; 3—catalog possible fraud symptoms; 4. Use technology to gather data about symptoms; 5. Analyze results, and 6. Investigate symptoms. Internal controls are part of a proactive system against fraud and are viewed as effective anti-fraud measures designed to prevent unauthorized transactions and activity and to ensure early detection (33).

Internal Audit

The Institute of Internal Audit defined internal auditing as an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. Its role includes detecting, preventing, and monitoring fraud risks and addressing those risks in audits and investigations. The role of the internal audit is to support the leadership of an organization by providing insights that can help them manage their

operations more effectively. The internal audit team evaluates all the decisions made by the leadership to ensure that they facilitate the smooth and efficient functioning of the organization. The primary goal of the internal audit is to generate additional value for the organization (34).

Types of Audit data analytic Software tools

There are a variety of tools/vendors available to perform data analytics. The most popular are Desktop Excel, Access; Server-based (SQL); Integrated –SAP, People Soft, JDE, Oracle; Report Writers – Business Objects, Cognos; Specialized Auditing Software, IDEA, SAS, Artu bus, ACL and Specialized DA Visualization Software Tableau, QlikView/Qlik Sense. Microsoft Access and Excel are the primary tools for data preparation and analysis, with additional reliable options such as IDEA, Minitab, and Sigma Plot for producing complex graphs (35). Organizations use forensic data analytics tools, but lower adoption of more sophisticated Forensic data analytic (FDA) tools, which constituted 65% of survey participants report using spreadsheet tools such as Microsoft Excel and 43% report using database tools such as MS Access or MS SQL Server. While these tools are essential to every FDA program, they often focus on the matching, grouping, ordering, joining or filtering of primarily descriptive data (11).

Results

Response Rate

Out of 55 distributed questionnaires, 44 responses were received, representing 80 percent of the targeted internal auditors. At the same time, there was a target of 10 internal auditors for interviews, but seven responded to the interview invitation. The need for internal auditors to prevent and detect fraud using data analytic tools could also have affected the response rate. Data collected from the questionnaire was analyzed using Microsoft Excel.

Table 1: Respondents' demographic information (n = 44)

Gender	**Frequency**	**Percent**
Male	34	77.3
Female	10	22.7
Age	**Frequency**	**Percent**
Less than 29	9	20.5
30-39	14	31.8
40-49	16	36.4
50-59	4	9.1
Above 60	1	2.3
Experience	**Frequency**	**Percent**
0-10	19	43.2
11-20	16	36.4
21-30	7	15.9
More than 30	2	4.5
Educational Qualification	**Frequency**	**Percent**
Diploma	3	6.8
Degree	8	18.2
Postgraduate	17	38.6
Professional Certification [CFE, CA, IIA, ACCA, CGI(CIS), Other]	16	36.4

The demographic profile of the respondents has been summarized in Table 1. The first section of the Questionnaire explored the demographic data: Gender, age of respondents, education qualification, and experience of the internal auditors. Out of the 44 respondents, the majority of the respondents were male, constituting thirty-four respondents, followed by the females, which represented 10 respondents. Their age group produced a finding showing that most respondents were relatively young. The distribution indicates that the highest number of respondents falling in the age range of 40-49 is sixteen respondents, while the lowest was above 60 years and had only one respondent. The table shows that the respondents are relatively less experienced in internal auditing.

Most respondents had experience in 0-10 years, which is nineteen respondents, followed by 11-20 years, which is sixteen respondents. Fewer respondents had 21-30 years of experience is seven respondents, and only two respondents had more than 30 years of experience. The level of education and professional certification was relatively high. The highest number of respondents who had post-graduate qualifications was seventeen respondents, followed by professional accreditation, which was sixteen respondents, then degree and diploma, which had eight and three respondents, respectively.

Table 2: Asset Misappropriation

	Skimming	**Cash Larceny**	**Billing Fraud**	**Expense Reimbursement Fraud**	**Payroll Fraud**	**Inventory Theft.**	**Mean**
Strongly Disagree	2	3	2	-	-	-	1
Disagree	2	-	1	-	-	1	1
Neutral	5	1	1	1	1	1	2
Agree	19	21	22	30	24	24	23
Strongly Agree	16	19	18	13	19	18	17
Total	44	44	44	44	44	44	44

Table 2 presents the types of asset misappropriation internal auditors have encountered. This table caters for insights into specific forms of asset misappropriation that are commonly addressed. The mean analysis presented by the table indicates that 23 and 17 respondents agreed and strongly agreed, respectively, that fraud analytics assist in identifying various types of asset misappropriation, such as skimming, cash larceny, billing fraud, expense reimbursement fraud, and inventory theft.

Table 3: Financial Statement Frauds

	Strongly Disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**	**Total**
It is easy to identify Timing Differences without fraud analytics	2	14	11	13	4	44
It is easy to identify Fictitious Revenue without fraud analytics	2	21	5	8	8	44
It is easy to identify Understated Revenue without data analytics	0	26	7	6	5	44
It is easy to identify Concealed Liabilities and Expenses without fraud analytics	2	27	5	7	3	44
It is easy to identify Overstated Liabilities and Expenses without fraud analytics	1	21	8	13	1	44
It is easy to identify improper Asset valuations without fraud analytics	2	19	10	7	6	44
It is easy to identify improper disclosures without fraud analytics	3	18	6	15	2	44
Mean	2	21	7	10	4	44

Table 3 shows the need for data analytics to detect and prevent financial statement fraud. Most of the internal auditors disagreed with the assumption that it is easy to find financial statements without data analytics tools, and on average, there were 21 who disagreed, and 2 strongly disagreed. A total of 10 and 4 agreed and strongly agreed, respectively. Only 7 of the respondents were neutral. This shows that most respondents agree that fraud analytics is needed to identify fraud.

Table 4: Data Analytic Software Used by Organizations

Software		Frequency	Percent	Valid Percent	Cumulative Percent	Mean	Std. Deviation
Microsoft Excel	Used	44	100	100	100	1.00	0.000
	Not Used	-	-	-	-	-	-
ACL	Used	18	40.9	40.9	40.9	1.59	0.497
	Not Used	26	59.1	59.1	100	-	-
IDEA	Used	19	43.2	43.2	43.2	1.57	0.501
	Not Used	25	56.8	56.8	100	-	-
Microsoft Power BI	Used	18	40.9	40.9	40.9	1.59	0.497
	Not Used	26	59.1	59.1	100	-	-
Python	Used	10	22.7	22.7	22.7	1.77	0.424
	Not Used	34	77.3	77.3	100	-	-
R	Used	6	13.6	13.6	13.6	1.86	0.347
	Not Used	38	86.4	86.4	100	-	-
Tableau	Used	12	27.3	27.3	27.3	1.73	0.451
	Not Used	32	72.7	72.7	100	-	-
	Total	44	100	100	-	-	-

The questionnaire required the respondents to respond to the different types of data analytic software applied within their organization, including hardware, cloud computing, and data security. Data analytic software used by organizations Table 4 shows the frequency and percentage of respondents using each software tool. Microsoft Excel shows that it is extensively used, with usage of 100% and a mean of 1, indicating usage by every participant. 43% of the respondents reported using IDEA, while ACL and Power BI had 41% of respondents using the software. The mean for IDEA was 1,57, while for ACL and Power BI was 1.59, showing moderate usage of both tools. Tableau, Python, and R used 27%, 21%, and 14%, respectively. The three data analytic software show moderate usage; their mean ranged between 1.73 and 1.86.

Table 5: Types of Hardware Used

Data Analytic Hardware	Used	Not Used
Computers	100%	0%
Servers	100%	0%
Storage Systems [HDD, SSD, NAS (Network Attached Storage)]	86%	14%
Mobile Devices	98%	2%
Peripherals (Monitors, Printers, Photocopier, Scanners)	100%	0%

Table 5 shows respondent results on the hardware they use within their organizations. The respondents indicated that they all use computers, servers, and peripherals. Respondents revealed that 86% used various storage systems such as hard disk drives (HDD), Solid state drives (SDD), and Network attached storage for data analytics. The data shows that 98% use mobile devices for data analytics.

Table 6: Cloud Computing

	Used	Not Used
AWS	15	29
Microsoft Azure	14	30
Google Cloud	31	13
Mean	20	24

Table 6 displays the cloud computing usage of the respondent organization. The findings indicate that Google Cloud is the most widely used cloud platform among the respondents, with 31 organizations utilizing it. Many respondents used Microsoft Azure and AWS, with 14 and 15 users, respectively. The mean values of 24 respondents who did not use the cloud platform compared to those who used 20. This could imply that cloud adoption is prevalent, but some respondents still have not adopted cloud computing services. Table 5 provides types of cloud computing used by internal auditors.

Table 7: Data Security and Governance

		Frequency	Per cent	Valid Percent	Cumulative Percent
Data Access Controls	Used	42	95.5	95.5	95.5
	Not Used	2	4.5	4.5	100.0
Data Encryption	Used	36	81.8	81.8	81.8
	Not Used	8	18.2	18.2	100.0
Data Masking	Used	26	59.1	59.1	59.1
	Not Used	18	40.9	40.9	100.0
	Total	44	100.0	100.0	-

Table 7 shows the respondents' data security and governance results. Data collected from clients is often sensitive and requires integrity and confidentiality. In an analysis of security data, the responses were high in the use of data security. They were topped by data access controls, which had 42 responses out of 44, followed by data encryption, of which those who highlighted usage were 36, and only eight were not using encryption. Twenty-six respondents and 18 respondents used data masking that they were not using.

Table 8: Appreciation for Adopting the Use of Data Analytic Tools

	n	Mean	Standard Deviation
Organizations understand the potential benefits of using data analytics tools.	44	3.82	.815
Organizations have invested sufficient resources to adopt data analytics tools.	44	2.70	1.025
Organizations have a clear understanding of how to use data analytics tools effectively.	44	3.11	.945
Organizations have a culture that supports the use of data analytics tools.	44	3.11	.993
Organizations have a clear data analytics strategy aligning with their goals and objectives.	44	3.20	.978
Organizations have sufficient data quality to use data analytics tools effectively.	44	3.11	1.061
Organizations have access to the necessary data analytics tools.	44	3.11	1.039
Organizations have the necessary talent to use data analytics tools effectively.	44	3.25	.866
Organizations have experienced positive results from using data analytics	44	3.68	.934
Organizations plan to increase their adoption of data analytics tools in the future.	44	3.93	.625

Table 8 summarizes the appreciation and plans for adopting data analytic tools among organizations. It shows that the respondents, on average, rated appreciation for adopting data analytics by organizations at a high of 3.93, and the lowest was 2.97. The standard deviation also had a range of 0.625 and 1.061. This shows that organizations generally recognize the potential benefits of using data analytic tools. There are areas that organizations should look into, such as resource allocation, understanding how to effectively use the tools and a culture of how to use the tools. Resource allocation showed that internal auditors were not receiving adequate resources, and most respondents disagreed with the organization's investment in sufficient tools.

Discussion

Discussion of Data Analytic Tools That Internal Auditor Can Use

Occupational Fraud in Organizations

Proactive internal auditors have outlined a six-step approach to detect occupational fraud, involving the identification of potential frauds, gathering data on symptoms using technology, and conducting thorough investigations. The findings show that overall, the combination number of respondents who agree and strongly agree (23+17=40) shows a positive sentiment towards the effectiveness of fraud analytics in addressing asset misappropriation. The financial statement frauds also showed that data analytics are helpful in identification.

Data Analytic Software, Hardware, Cloud Computing, Security

Microsoft had the highest usage among the respondents; the other usage tools vary, with ACL, IDEA, and Microsoft Power BI having similar usage levels, while Python, R, and Tableau had lower usage rates. These findings provide insights into the popularity and adoption of different software tools among the surveyed population. The most used data analytics tools are spreadsheet tools such as Microsoft Excel, which constitute 65% of the total.

Cloud Computing

The findings from cloud computing show that it has become a primary-stream technology with significant adoption among respondents. Google Cloud, Microsoft Azure, and AWS are prominent players in the cloud market, attracting users for various reasons. Indications show that some internal auditors still have not adopted cloud services, which shows that considerations and challenges must be addressed for wider adoption. From a proactive point of view, internal auditors should work with the IT department and other departments that use cloud applications to ensure that their agreements with service providers contain an audit requirement or include reporting on the controls used.

Data Governance and Security

These security measures play a crucial role in safeguarding sensitive information and protecting data from unauthorized access, making them essential components of robust data security practices. The security measures ensure that during transmission and when stored in a database or cloud, data remains protected and, if intercepted, remains unreadable and secure. According to their responses, the internal auditors have embraced data access and encryption, showing high usage between 81% and 95%. By analyzing the security of data in the organization, auditors can identify potential risks, assess compliance, and make recommendations to enhance the organization’s overall security posture and protect sensitive information effectively.

Critical Analysis of Findings

The findings from the study reveal significant insight, and it is the first attempt at integrating Fraud Data Analytics in combating occupational fraud within Zimbabwean listed companies. The analysis indicates that Fraud Data Analytics can significantly enhance the capabilities of internal auditors. There are some challenges as well, and to address these challenges, investment in the latest tools is required. Continuous training is also necessary for internal auditors to achieve proper results.

Actionable Strategies to overcome challenges in Fraud Data Analytics

In the current scenario, adapting Fraud Data Analytics is very important for identifying occupational fraud at the early stages. Companies should organize regular workshops and training for auditors on Fraud Data Analytics to overcome the challenges. Further, companies should procure user-friendly software that can help with faster analysis. Management should highlight the requirement for Fraud Analytics in organizations. Management should invest more in Artificial

Intelligence and Machine Learning to achieve this objective. Further, Management of companies should foster a continuous learning environment to encourage auditors to learn new Forensic Accounting and Fraud Investigation tools. In addition, organizations should use blockchain technology, AI, and ML to prevent fraud in the early stages.

Interview Findings and Discussion

The interviewees responded to the following questions that the interviewer had asked during the interview.

Which data analytic tools are used by internal auditors within your organization to detect and prevent fraud?

Of the seven interviewees, the three respondents highlighted that they are using Microsoft Excel, Transaction software, ACL, and ERP tools such as SAP, High Bond, and Teammate to analyse data within their organisation. Out of all the seven, only one showed that they used Benford's law in analysing financial data presented to them. The rest said they mainly rely on Microsoft Excel as it is readily available. The reason for not using Benford's law is the lack of awareness among internal auditors.

What are the roles of internal audits in preventing and detecting asset misappropriation?

The following roles for internal auditors were provided by the seven interviewees: risk assessment, ensuring compliance with internal controls and established procedures, acting as advisors to management through reporting and communication via report writing, and the prevention and detection of fraudulent activities (32). These roles align with a study indicating that the internal audit function is intended to support an organization's leadership by providing insights to help manage operations more effectively. The internal audit team evaluates all the decisions made by the leadership to ensure that they facilitate the smooth and efficient functioning of the organisation. The primary goal of the internal audit is to generate additional value for the organisation.

State internal auditors' other challenges when adopting data analytic tools

Five out of seven internal auditors highlighted that the reason for not fully adopting data analytic tools was the lack of know-how fraud analytic tools. Most are used to traditional software such as Microsoft Excel. They also highlighted that there is a lack of skill and competency. At most, there is a lack of funding from management, which is unwilling to support the implementation of data analytic tools.

Further Scope of Research

The study results show a significant correlation between preventing and detecting asset misappropriation through data analytic tools. Research can be done to verify if data analytic tools can be applied to fraud and corruption in financial statements. In the future, a study of the effectiveness of forensic auditing in detecting and preventing asset misappropriation of Zimbabwe-listed companies may be carried out.

Limitations of The Study

The research study looked at the tools that internal auditors can utilise to prevent and detect asset misappropriation. The main limitation was that the study researched the internal audit and excluded the forensic accountant and the external auditors. The researcher did not cover the whole occupational fraud but focused mainly on asset misappropriation and did not cover corruption and financial statement fraud. The study did not look at cases that involved crimes against the organisation by outsiders.

Conclusion

The analysis showed that the internal auditors' most used software data analytics tool in preventing and detecting asset misappropriation is Microsoft Excel, which revealed that all have access to the software. Organizations must invest in other data analytic software such as ACL, Tableau, Power BI, and IDEA. This software assists internal auditors by enhancing their data analysis capabilities, improving visualisation and reporting, increasing efficiency, and identifying potential risks and fraudulent activities. The conclusion that can be drawn from this analysis is that internal auditors would have to consider the use of multiple tools and techniques in fraud detection to complement and strengthen each other's capabilities. Implementing the roadmap for advanced tools like ACL, Tableau, Power BI, and IDEA to advance data analysis capabilities can be done in four phases. In phase 1, an Evaluation of the current infrastructure is required and should understand the requirements of organizations. In Phase 2, Testing the advanced tools in the controlled environment

can help to meet organisation requirements. In Phase 3, tools should be installed in the organisation to train the employees. Phase 4 Continuous monitoring and improvement are required to optimise and address the issues. This four-phase implementation can help save significant amounts that could be lost to fraud. To adopt advanced tools and policy, policymakers should start working systematically and emphasise adopting fraud prevention, creating a culture of accountability and transparency. Lastly, Data analytics plays a vital role in detecting and preventing fraud, and organisations are exploring data analytics to enhance their capabilities. By leveraging data analytics, internal auditors can efficiently correlate and analyse vast volumes of electronic data from various sources. This enables faster and more comprehensive analytics, empowering them to identify fraudulent activities more effectively and take proactive measures to prevent and mitigate fraud. Internal auditors face various challenges when it comes to utilising data analytics. The challenges faced include hiring and retaining talent, aligning strategies with organisational goals, data quality and consistency, integrating tools with existing systems, ensuring data security and privacy, obtaining buy-in from stakeholders, identifying appropriate tools and techniques, ensuring user-friendliness and measuring effectiveness and return on investment. These challenges require careful consideration and proactive efforts to overcome, allowing internal auditors to harness the full potential of data analytics in their audit process.

Abbreviations

ACFE: Association of Certified Fraud Examiners, ACL: Audit Command Language, IDEA: Interactive Data Extraction and Analysis, SQL: Structured Query Language, SAP: Systems Applications and Products in Data Processing, ERP: Enterprise Resource Planning, Power BI: Power Business Intelligence

Acknowledgements

Nil.

Author Contributions

Conceptualization: Himanshu Thakkar and Gudoshava Chrispen Fanuel, Methodology: Himanshu Thakkar; Validation: Saptarshi Datta, Priyam Bhadra and Siddharth Baburao Dabhade; Formal analysis: Himanshu Thakkar; Investigation: Gudoshava Chrispen Fanuel; Resources: Gudoshava Chrispen Fanuel.; Data curation: Gudoshava Chrispen Fanuel.; Writing—original draft preparation: Gudoshava Chrispen Fanuel and Himanshu Thakkar; Writing—Review and editing: Gudoshava Chrispen Fanuel, Saptarshi Datta, Priyam Bhadra and Siddharth Baburao Dabhade; Visualization: Himanshu Thakkar; Supervision: Himanshu Thakkar.

Conflicts of Interest

The authors declare that they have no competing interests.

Ethics Approval

Nil.

Funding

This research received no external funding.

References

1. Bekiaris M, Efthymiou T, Koutoupis AG. Economic crisis impact on corporate governance & internal audit: The case of Greece. Corporate Ownership and Control. 2013;11(1):55–64.
2. El-Sayed Ebaid I. Internal Audit Function: An exploratory study from Egyptian listed firms. International Journal of Law and Management. 2011 Mar 22;53(2):108–28.
3. Macailao MC. The Internal Auditors on Occupational Fraud: An Integrative Literature Review. The Journal of Business, Tourism, Public and Legal Management. 2021 Jun;1(1):1–15.
4. Hayes A. The rise and fall of Worldcom: Story of a scandal. Investopedia; 2024. Available from: https://www.investopedia.com/terms/w/worldcom.asp
5. Chitemba B. Noczim prejudiced of US$16M. The Sunday Mail; 2015. Available from: https://www.sundaymail.co.zw/noczim-prejudiced-of-us16m
6. Kawadza S. Psmi falls on hard times, faces collapse. The Zimbabwe Independent; 2022. Available from: https://www.newsday.co.zw/theindependent/local-news/article/200003017/psmi-falls-on-hard-times-faces-collapse
7. Muzavazi. Fired NRZ executives fingered in US$30 000 scandal. 2020. Available from: https://zwnews.com/fired-nrz-executives-fingered-in-us30-000-scandal/
8. Muonwa J. Prominent Harare businessmen up for US$1.4 million fraud following shady property deal. https://www.newzimbabwe.com/. New Zimbabwe: The Zimbabwe News You Trust; 2024 Sep 30; Available from: https://www.newzimbabwe.com/prominent-harare-businessmen-up-for-us1-4-million-fraud-following-shady-property-deal/
9. Zdenka P, Petr S, Radek S. Data analysis: Tools and methods. In: Recent Researches in Automatic Control - 13th WSEAS International Conference on Automatic Control, Modelling and Simulation, ACMOS'11 2011, p 201-206. Lanzarote, Canary Islands: TBU

Publications; 2011. p. 201–6. Available from: https://publikace.k.utb.cz/handle/10563/1004758?locale-attribute=en
10. Zakir J, Seymour T, Berg K. Big Data Analytics. Issues In Information Systems. 2015;16(2):81–90.
11. Gepp A, Linnenluecke MK, O'Neill TJ, Smith T. Big Data Techniques in Auditing Research and practice: Current trends and future opportunities. Journal of Accounting Literature. 2018 Feb 1;40(1):102–15.
12. Bănărescu A. Detecting and preventing fraud with data analytics. Procedia Economics and Finance. 2015;32:1827–36.
13. Kudanga D, Mthombeni A, Chihongwa E, Singende M. The Role of Technology in Evidence Gathering for Cases of Fraud: Case of Bulawayo Central Business District, Zimbabwe. LIGHTHOUSE: The Zimbabwe Ezekiel Guti University Journal of Law, Economics and Public Policy. 2022; 1(1 & 2).: 22-41.
14. Dennis ME. The Role of Internal Auditor in Preventing Fraud. 2016. Available from: http://scholar.unand.ac.id/id/eprint/3030
15. Thakkar H, Datta S, Bhadra P, Barot H, Purohit M, Dabhade S. A bibliometric analysis of forensic accounting research: Unveiling its impact on tax fraud detection in SAARC countries. Journal of Informatics Education and Research. 2024;4(2): 2122-2131.
16. Lukman RP, Chariri A. The role of internal auditors in fraud prevention and detection: empirical findings from general banking. Diponegoro Journal of Accounting. 2023 Jan;12(1): 1-12.
17. Johnson GG, Rudesill CL. An investigation into fraud prevention and detection of small businesses in the United States: Responsibilities of auditors, managers, and business owners. Accounting Forum. 2001 Mar;25(1):56–78.
18. Moore J. Occupational Fraud Models: A Comparative Analysis and Proposed Expanded Model. International Journal of Accounting Research . 2020 Jun 10;8(2):1–5.
19. IAASB. 2020 Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements. International Federation of Accountants (IFAC); 2021.
20. Crawford RL, Weirich TR. Fraud guidance for corporate counsel reviewing financial statements and reports. Journal of Financial Crime. 2011 Oct 11;18(4):347–60.
21. Barney J. Firm Resources and sustained competitive advantage. Journal of Management. 1991 Mar;17(1):99–120.
22. Alqudah H, Amran NA, Hassan H, Lutfi A, Alessa N, alrawad M, et al. Examining the critical factors of internal audit effectiveness from internal auditors' perspective: Moderating role of extrinsic rewards. Heliyon. 2023 Oct; 9(10): 1-17.
23. Amoako GK, Bawuah J, Asafo-Adjei E, Ayimbire C. Internal audit functions and sustainability audits: Insights from manufacturing firms. Cogent Business & Management. 2023 Mar 19;10(1): 1-21.
24. Corazza L, Cottafava D, Torchia D, Dhir A. Interpreting stakeholder ecosystems through relational stakeholder theory: The case of a highly contested megaproject. Business Strategy and the Environment. 2023 Oct 29;33(3):2384–412.
25. Parmar BL, Freeman RE, Harrison JS, Wicks AC, Purnell L, de Colle S. Stakeholder Theory: The State of the Art. Academy of Management Annals. 2010 Jan;4(1):403–45.
26. Kotb A, Elbardan H, Halabi H. Mapping of internal audit research: A post-Enron Structured Literature Review. Accounting, Auditing & Accountability Journal. 2020 Aug 4;33(8):1969–96.
27. Kalovya OZ. Determinants of occupational fraud losses: Offenders, victims and insights from fraud theory. Journal of Financial Crime. 2020 Jan 29;30(2):361–76.
28. Delgado Y, Price BS, Speaker PJ, Stoiloff SL. Forensic intelligence: Data analytics as the bridge between Forensic Science and Investigation. Forensic Science International: Synergy. 2021;3:100162.
29. Khamainy AH, Amalia MM, Cakranegara PA, Indrawati A. Financial statement fraud: The predictive relevance of fraud hexagon theory. Journal of Accounting and Strategic Finance. 2022 Jun 30;5(1):110–33.
30. Achmad T, Ghozali I, Pamungkas ID. Hexagon fraud: Detection of fraudulent financial reporting in state-owned enterprises Indonesia. Economies. 2022 Jan 1;10(1):13.
31. Odeyemi O, Ibeh CV, Mhlongo NZ, Asuzu OF, Awonuga KK, Olatoye FO. Forensic accounting and fraud detection: A review of techniques in the Digital age. Finance & Accounting Research Journal. 2024 Feb 14;6(2):202–14.
32. Silverstone H, Sheetz M, Pedneault S, Rudewicz F. Forensic accounting and fraud investigation for Non-Experts. Hoboken, New Jersey: John Wiley & Sons Incorporated; 2012.
33. Petraşcu D, Tieanu A. The role of Internal Audit In Fraud Prevention and Detection. Procedia Economics and Finance. 2014 Dec 17;16:489–97.
34. Nigrini MJ. Forensic analytics: Methods and techniques for forensic accounting investigations. Hoboken, New Jersey: Wiley; 2011.
35. Abdulmunim O. Cloud accounting in Jordanian public shareholding companies: The Role of Internal Audit. Corporate Ownership and Control. 2018;15(4–1):158–64.