Forensic Secretarial Audit and Fraud Detection: Emerging Tools and Techniques for Practicing Company Secretaries

In light of the increasing incidence of compliance irregularities, corporate fraud, and governance failures, forensic secretarial audit (FSA) is emerging as an important governance tool integrating investigative scrutiny, compliance verification, and fraud detection within corporate governance systems. In this backdrop, this study examines the conceptual foundations of FSA, the nature of corporate fraud and governance vulnerabilities, and the growing role of Practicing Company Secretaries in preventive governance and forensic compliance assurance.

Dr. J. Madegowda
Former Professor (Kuvempu University), Mysuru
madegowdaj1@gmail.com

INTRODUCTION

Over the last two decades, corporate governance has undergone significant transformation with the growing incidence of corporate fraud, accounting manipulations, regulatory violations, and technological disruptions. High-profile corporate scandals have highlighted the shortcomings of traditional compliance-based auditing strategies in detecting sophisticated fraud schemes, governance manipulation, hidden related-party transactions, and digitally-enabled irregularities (Rezaee & Riley, 2022). Fraud is more complex, technologically sophisticated, and multidimensional in today's corporate landscape, which features complex financial models, cross-border transactions, integrated digitized systems and changing governance demands. Therefore, governance mechanisms are moving from "reactive verification of compliance" to "proactive and preventive assurance of governance mechanisms" (Haddad et al., 2024).

Traditional secretarial audit is primarily concerned with procedural compliance and statutory adherence. While this mechanism is still central to regulatory governance, it is frequently insufficient to detect intentional acts of regulatory failure, document tampering, compliance manipulation, or cyber-enabled misconduct (Bhasin, 2016). This shortcoming has led to the development of forensic techniques in corporate governance that integrate investigative techniques, analytics, digital forensics, and evidentiary analysis in the detection of fraud and governance risk assessments (Singleton & Singleton, 2010). Forensic secretarial audit (FSA) denotes the convergence of secretarial oversight, forensic accounting methodologies, and advanced technological skills to identify, investigate, and prevent governance violations and financial misconduct (Haddad et al., 2024).

The rapid development of the digital economy has further complicated compliance environments and fraud detection systems. Although the growing use of electronic records, cloud-based systems, e-filings, digital signatures, artificial intelligence (AI), and automated compliance systems has enhanced governance efficiency, it has also raised cyber-related vulnerabilities (Kokina & Davenport, 2017). Therefore, contemporary auditing should combine data analytics, digital forensics, and AI to tackle increasingly sophisticated fraud mechanisms (Oluwatosin et al., 2024). In this changing world, Practicing Company Secretaries (PCS) are becoming crucial governance professionals who not only ensure compliance but also strengthen preventive fraud surveillance and forensic governance oversight. In this context, this paper explores the increasing importance of FSA as a newly emerging governance instrument for fraud detection and compliance assurance.

CONCEPTUAL FRAMEWORK OF FSA

As businesses evolve, the volume of digital transactions, governance processes, and business operations have made audit and compliance tasks far more complex. Growing corporate fraud, governance failures, regulatory evasions, and technologically advanced misconducts have led to forensic approaches where investigative scrutiny is coupled with evidentiary analysis. "Forensic audit" denotes a specific type of investigation of financial, operational, and compliance issues to identify misconduct and fraud, and to provide legally admissible evidence (Singleton & Singleton, 2010).

"FSA" refers to a systematic and investigative examination of a company's secretarial, compliance, and governance records for investigating, detecting, and preventing fraud, breaches of fiduciary duty, and governance violations (Almasria, 2022). It is a hybrid approach that uses investigative techniques designed for forensic accounting,

digital forensics, and governance analytics to expose concealed fraud schemes, hidden transactions, and governance anomalies. Primarily, FSA is a preventive, investigative, and governance-based approach. It is more than just procedural verification; it looks at the intentions, integrity and authenticity of corporate actions and disclosures. It involves scrutiny of board proceedings, regulatory filings, statutory registers, related-party approvals, digital communication systems, and electronic records to identify irregularities, unauthorized transactions, and policy violations (Haddad et al., 2024). It ensures the preservation and examination of digital and documentary evidence for use in litigation, regulatory inquiry and enforcement actions (Kaawaase et al., 2021). It also enhances internal controls, stakeholder confidence, ethical governance practices and organizational transparency.

Shell entities, layered transactions, disguised ownership, and digital manipulation are increasingly used by organizations to conceal fraudulent activities and evade regulatory oversight (Rezaee & Riley, 2022). Moreover, statutory record falsification, board resolution manipulation, use of digital signatures, and covering up related-party transactions are significant governance issues. The rapid digitalization has further increased vulnerabilities associated with electronic documentation, fraud enabled by digital technology, and unauthorized record modifications (Familoni, 2024). Common compliance audits may not have the investigative techniques necessary to uncover those advanced irregularities. The expectations of all stakeholders and the watchful eye of regulatory bodies like the Securities and Exchange Board of India (SEBI), the Ministry of Corporate Affairs (MCA), the Serious Fraud Investigation Office (SFIO), etc., have intensified significantly (Kaawaase et al., 2021). Against this context, FSA has emerged as a niche governance process that can combine compliance verification with forensic investigation and technology-based fraud detection processes.

> Improving digital compliance infrastructure, secure audit trails and integrated governance systems will thus be critical to further improve fraud detection capabilities and governance resilience in future corporate ecosystems.

CORPORATE FRAUD AND GOVERNANCE VULNERABILITIES

The growing sophistication of corporate fraud has exposed important weaknesses in traditional governance and compliance systems. Understanding these vulnerabilities is, therefore, necessary for strengthening forensic governance mechanisms.

a. Nature of Corporate Fraud

"Corporate fraud" refers to any dishonesty conducted by an insider/outsider of an organization to gain a financial or strategic advantage at the cost of the organization's fiduciary duties, governance practices or legal responsibilities (Haddad et al., 2024). Corporate fraud has become more complex due to the increasing sophistication of corporate operations, digital transactions and governance systems. Contemporary fraud is not limited to traditional accounting fraud; they increasingly involve governance engineering, technological abuse, regulatory evasion, and cyber-enabled misconduct.

Financial statement fraud is one of the most problematic types of corporate fraud, involving intentional misrepresentation of financial items, or accounting records to deceive investors, regulators and other stakeholders (Rezaee & Riley, 2022). It often includes revenue inflation, concealment of liabilities, fictitious transactions, and/or altering financial statements. Besides, directors, executives, or employees may use their position for personal gain by insider trading, diverting corporate assets, engaging in conflict-of-interest transactions, or falsely disclosing.

Manipulating governance is a frequent tactic in corporate fraud, with falsified statutory registers, altered board minutes, backdated resolutions, and fake approvals designed to create the impression of procedural legitimacy. Furthermore, compliance fraud like false certificates, misleading regulatory filings, and deliberate non-disclosures have surfaced as major governance issues in highly regulated business environments. Corporate processes have been digitized at a fast pace, making cyber-enabled fraud even more prevalent. Unauthorized access to governance systems, manipulation of electronic records, phishing attacks, ransomware incidents, use of digital signatures and fraudulent digital transactions have significantly increased the complexity of governance risk management and fraud detection mechanisms (Familoni, 2024).

b. Governance Failures and Compliance Gaps

Internal control weaknesses, inadequate separation of duties, and lack of oversight and compliance monitoring systems provide opportunities for manipulation and cover-up of irregularities (ACFE, 2024). Governance frameworks often fail due to excessive managerial dominance, passive directorship, lack of professional skepticism, and/or insufficient board independence (Kaawaase et al., 2021). However, there are many compliance gaps, including inadequate disclosure systems, insufficient whistleblowing procedures, insufficient compliance training, and the absence of integrated risk assessment frameworks (Almasria, 2022).

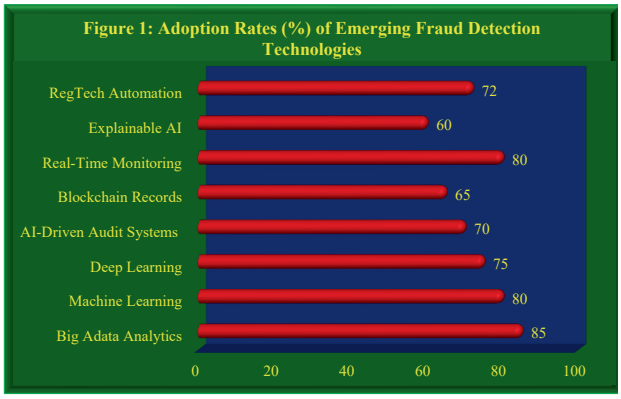
c. Red-Flag Indicators in Secretarial and Compliance Records

FSA is crucial for uncovering red flags in governance processes and compliance documentation. Some

abnormalities signal that there is hidden dishonesty and need further in-depth investigation by the forensic process. Examples include backdated resolutions, discrepancies between internal records and Registrar of Companies (ROC) filings, repetitive changes in the statutory registers, or the lack of evidence of quorum and dissent (Almasria, 2022). Likewise, unusual related-party approvals without supporting documentation, unapproved changes to governance policies, and major transactions just prior to reporting periods are potential red flags. Major forensic issues in digital signature systems include misuse of digital signatures, destruction or alteration of electronic records, unauthorized access to systems, and lack of audit trails (Familoni, 2024). These red flags do not happen in isolation, but rather stem from many interrelated governance shortcomings that can only be examined through a technology-assisted forensic and investigative analysis.

EMERGING FRAUD DETECTION TOOLS AND TECHNOLOGIES

Digitalization has also transformed the way corporate governance systems are conducted and the way in which fraud is detected and compliance managed. The technology of surveillance, automated monitoring tools and data-driven investigation processes are increasingly part of contemporary governance environments to detect irregularities that lie undetected in a traditional audit environment. In this evolving context, new technologies are now playing a significant role in not only augmenting the FSA process but also in facilitating PCS to detect governance anomalies, compliance manipulation, and fraudulent activities in real time (Kokina & Davenport, 2017). The use of AI, digital forensics, blockchain systems, Regulatory Technology (RegTech) solutions, cybersecurity frameworks, and cloud-based platforms for governance has greatly broadened the range and capabilities of corporate fraud detection processes (Figure 1).



Source: *(Haddad et al., 2024; Oluwatosin Ilori et al., 2024)*

a. AI and Data Analytics in Fraud Detection

The use of AI and machine learning technologies has transformed fraud detection by being able to analyze large amounts of data, detect anomalies and hidden patterns that are typical of fraudulent activity. These AI-based systems can analyze both unstructured and structured data to detect suspicious transactions, irregular compliance filings, unusual approval workflows, and other deviations from standard governance protocols. The accuracy for fraud detection with the machine learning algorithms is reported to be very high and the false positive rate is significantly lower compared to traditional rule-based methods.

Supervised learning algorithms, such as clustering and anomaly detection algorithms, help in identifying emerging fraud patterns and statistical outliers that deviate from normal behavior patterns (Oluwatosin et al., 2024). Deep learning systems detect suspicious language, hidden coordination, or governance issues in emails, narrative documentation, and communication patterns. Explainable AI (XAI) methods are also becoming significant as they help auditors and governance practitioners to understand and verify algorithmic findings. The use of predictive analytics is a powerful way to improve proactive fraud prevention by predicting high-risk transactions or governance activities before misconduct occurs (Oluwatosin Ilori et al., 2024).

b. Digital Forensic Tools

In an electronically managed corporate environment, digital forensic technologies are invaluable tools of FSA. "Digital forensic" is the systematic process of collecting, preserving and analyzing electronically stored evidence as per legal and evidentiary framework (Malik et al., 2024). Metadata analysis assists investigators to gain access to information that is not immediately obvious from the text of an electronic document, such as its authorship information, modification history, timestamps and access records. This can uncover document tampering, unauthorized changes, and backdated resolutions. Furthermore, disk imaging, deleted file recovery, mobile device forensics, and cloud forensics will allow evidence to be recovered from digital infrastructure even after attempted deletion or concealment (Malik et al., 2024). Chain-of-custody documentation also helps to ensure that digital evidence is admissible in litigation and regulatory matters (Malik et al., 2024).

c. RegTech and Compliance Automation

"RegTech" represents any technology-based method for automating compliance monitoring, reporting and governance management tasks. RegTech solutions increasingly transform the practice environment of PCS through automated compliance dashboards, real-time reporting systems and integrated compliance tracking software. Automated transaction monitoring systems can compare financial transactions with compliance regulations and behaviour profiles to detect suspicious transactions linked with money laundering, sanction violations and/or fraudulent transactions. Real-time monitoring mechanisms for compliance enable ongoing monitoring of the organization's activities and compliance requirements,

thus allowing for the detection of breaches of the policy and governance deviations. Document management, compliance reporting, risk scoring, regulatory change tracking and due diligence processes are also automated on RegTech platforms.

d. Blockchain and Immutable Record Systems

In recent years, blockchain technology has gained considerable popularity in the field of governance and compliance management because of its ability to build a transparent, decentralized and tamper-proof record system (Haddad et al., 2024). Blockchain-based documentation systems provide immutable documentation, which is difficult to falsely manipulate or alter without being detected, thus minimizing the risk of unauthorized manipulation and falsification.

Smart contracts that are part of the blockchain infrastructure automatically implement governance processes and compliance checks in a coded authorization process. Accountability can be further enhanced with the use of multi-signature authorization systems, where the cryptographic signature of multiple authorized users is needed before governance decisions are executed (Haddad et al., 2024). Furthermore, blockchain systems can improve the traceability and credibility of evidence by providing a complete record of all changes to the evidence and governance activities (Dai & Vasarhelyi, 2017).

e. Cybersecurity and Fraud Surveillance Systems

Cybersecurity frameworks have become part of today's fraud detection systems. Intrusion detection systems, user behaviour analytics, endpoint detection solutions, and security information and event management (SIEM) platforms keep a constant watch on suspicious activities, unauthorized access attempts and abnormal behavior patterns within organizations. Data loss prevention systems also track sensitive data transfers and help to block unauthorized data exfiltration (Familoni, 2024). These are especially important for PCS for managing electronic records, virtual board meetings, approvals and cloud-based governance systems.

f. Cloud-Based Documentation and E-Governance Systems

There has been a complete shift in compliance management and governance documentation with cloud-based governance platforms. Centralized repositories of documents enable the real-time monitoring of the document, standardized record keeping and secure collaborative governance processes (Bernardo et al., 2024). Version control systems automatically maintain a history of document revisions, allowing identification of unauthorized changes and restoration of previous versions if needed (Malik et al., 2024). E-governance systems automate management of board meetings, document circulation, voting and compliance reporting to reduce opportunities for procedural manipulations (Bernardo et al., 2024). While cloud-based systems provide greater governance transparency and enhance operational efficiency, they must also have effective cybersecurity protections, encryption, and forensic monitoring systems to ensure that the data cannot be accessed by unauthorized parties, compromised, or destroyed (Table 1).

Table 1: Emerging Technologies for Fraud Detection and Their Relevance in Forensic Secretarial Practice

Tool/Technology	Application in PCS Practice	Fraud Detection Utility
AI and Machine Learning	Compliance analytics and behavioural monitoring	Detection of anomalies and suspicious patterns
Predictive Analytics	Governance risk forecasting	Early fraud risk identification
Digital Forensic Tools	Examination of electronic evidence	Detection of tampering and digital manipulation
RegTech Platforms	Automated compliance management	Continuous monitoring of compliance deviations
Blockchain Systems	Immutable governance records	Prevention of unauthorized alterations
Cybersecurity Surveillance	Monitoring digital governance systems	Detection of cyber-enabled fraud
Cloud-Based Governance Platforms	Centralized documentation and virtual audits	Enhanced transparency and evidentiary reliability

Source: *Compiled and constructed by the author based on relevant literature*

ROLE OF PCS IN FORENSIC GOVERNANCE

Beyond compliance functions, PCS increasingly contribute to governance surveillance, fraud prevention, and forensic assurance.

a. PCS as Governance Professionals

With the development of modern governance systems, PCS' roles are being more and more acknowledged as governance professionals charged with ensuring transparency, accountability, ethics, and regulatory compliance in organizations (Almasria, 2022). PCS occupy strategically pivotal positions within corporate governance because of their participation in the activities of boards, regulatory filings, corporate documentation and stakeholder communication (Kaawaase et al., 2021). They have ready access to confidential corporate information, board meetings

and the compliance records, which allow them to detect anomalies in governance and deviations from the usual procedures that may indicate fraud or misconduct (Almasria, 2022). In this context, PCS act as facilitators of ethical governance, upholding procedural integrity, responsible corporate practices, and establishing accountability mechanisms.

b. Investigative and Preventive Functions

PCS are positioned to evaluate unusual transaction structures, irregular approval processes, inconsistencies in filing and unusual governance practices that otherwise might go unnoticed (Almasria, 2022). Transaction analysis is a vital investigative area, looking at related-party transactions, board approvals, and key corporate decisions to uncover financial irregularities or unauthorized activities (Haddad et al., 2024). Analysis can also be used to uncover hidden communication or evidence of misconduct. PCS help support continuous compliance surveillance, governance risk assessment and internal controls that will prevent future wrongdoing. They are also key in due diligence processes linked to mergers, acquisitions, restructuring, and fundraising activities, uncovering hidden liabilities, governance issues, and compliance vulnerabilities. Preventive governance systems are further strengthened by whistleblower protection mechanisms, employee awareness programs, policy development initiatives and governance framework enhancement (Almasria, 2022).

c. Evidentiary and Reporting Responsibilities

Forensic governance investigations produce significant evidentiary and reporting responsibilities requiring PCS to maintain high standards of documentation and record preservation. Proper maintenance of board minutes, statutory registers, approvals, disclosures and compliance certifications promotes accountability and defensibility in the face of regulatory examinations or litigation (Haddad et al., 2024). An important role is to report irregularities, deviations in governance, and findings from investigations objectively. Reports should be clear and distinguish between the facts, analysis, and opinions, and should be confidential and adhere to evidentiary standards (Haddad et al., 2024). As regulatory compliance officers, they are becoming more of governance assurance officers, helping to build transparency and stakeholder trust in the organizations. Notably, PCS are required to develop expertize in digital governance management and forensic technology systems.

LEGAL AND REGULATORY DIMENSIONS

FSA in India is guided by legal and regulatory provisions as outlined in the Companies Act, 2013 and other regulations. For example, Section 204 of the Companies Act aims at strengthening governance accountability and compliance assurance for certain classes of companies. In this changing scenario, the role of the Company Secretary is increasingly coming under the microscope for implementing governance mechanisms that will help detect fraud risks and compliance abnormalities (Almasria, 2022).

The regulatory environment has also strengthened with the increased disclosure and governance provisions stipulated by SEBI, which put a greater emphasis on transparency, board accountability, disclosure of related-party transactions and on timely reporting, thus increasing the compliance and monitoring burden on PCS (Kaawaase et al., 2021). Other regulatory requirements for anti-money laundering, sanctions compliance and financial reporting impose a significant burden that nonetheless demands forensic governance review. The SFIO may undertake investigations in serious cases of fraud and manipulation of governance. The legal framework also includes provisions on falsification of records, concealment of material information, misstatements and wrongful disclosures, emphasizing the increasing significance of forensic compliance mechanisms. A new field of interest is digital evidence and data protection issues for governance investigations. Investigation procedures must also follow the rules of privacy protection, whistleblower protections, employment law rules and evidence as it relates to admissibility of digital evidence (Bernardo et al., 2024). Therefore, legal knowledge, forensic sensitivity and technical skills are becoming an increasing part of the legal landscape of today's secretarial practice.

CHALLENGES IN IMPLEMENTING FSA

Although FSA is becoming increasingly important in contemporary corporate governance, it presents many structural, technological and regulatory challenges.

(a) Lack of specialized training and interdisciplinary expertize among professionals is one of the major concerns. Forensic Secretaries should understand the principles of corporate law, governance and corporate systems, fraud investigation methods, digital forensics, cybersecurity and evidentiary protocols. But most compliance professionals are still trained mainly in traditional procedural compliance and not technology-driven investigative analysis. Lack of competencies in data analytics, digital investigation, and forensic skills continues to limit implementation capabilities (Haddad et al., 2024).

(b) There are also significant operational barriers due to technological constraints. High-tech fraud detection solutions come at a price and with specific technical skills (Bernardo et al., 2024). Integrated governance monitoring systems can be difficult for small and medium-sized organizations because of resource constraints and cost-benefit considerations (Almasria, 2022). Furthermore, a lack of or inadequate data can hinder the processes of analytical and forensic examination (Oluwatosin Ilori et al., 2024).

(c) Data privacy and confidentiality, as well as evidentiary issues, are other significant issues. During forensic investigations, access to sensitive company data, employee communications, electronic records and

confidential governance documents is often required. Organizations need to balance investigative needs with privacy, confidentiality requirements and rules of evidence relating to electronic documentation. Electronic evidence may be further complicated by regulatory uncertainty over how to investigate and adduce electronic evidence (Bernardo et al., 2024).

(d) Furthermore, there are practical challenges, such as management and organizational resistance, especially if senior executives or governance weaknesses are involved in the investigation (Almasria, 2022).

(e) Last but not the least, there is no specific regulatory structure for FSA that would allow for some standardization in regard to investigative methodology, reporting, and professional responsibility. Hence, there is a need for better institutional oversight, targeted training and professional standards to enhance the effectiveness and credibility of forensic governance practices.

CONCLUSION

Global governance systems are growing in sophistication, and corporate fraud is becoming more complex, requiring a more sophisticated FSA. Specialized forensic training program for PCS is one of the prerequisites. Given the increasing complexity of digital investigations, cyber-risk assessment, data analysis, and evidentiary examination in forensic governance, it is essential that professional education not only teaches students the traditional compliance-based competencies but also adopts an interdisciplinary perspective in teaching forensic competencies.

The development of specific forensic governance standards also needs to be addressed on priority basis. There is no consistent and uniform professional body to oversee the investigative method, the evidentiary process, documentation and reporting requirements. Clarification of professional guidance and best practices can be achieved through institutional support from the Institute of Company Secretaries of India, industry engagement and regulatory partnership.

Moreover, the importance of interdisciplinary collaboration among Company Secretaries, Forensic Accountants, Cybersecurity Professionals, Lawyers, and Data Scientists to address many of the challenges surrounding effective forensic governance is growing. Improving digital compliance infrastructure, secure audit trails and integrated governance systems will thus be critical to further improve fraud detection capabilities and governance resilience in future corporate ecosystems. Overall, FSA denotes an emerging commitment towards governance integrity, proactive fraud prevention, and sustainable corporate accountability in a growing digital business environment.

REFERENCES:

i. *ACFE. (2024). Occupational fraud 2024: A report to the nations. Association of Certified Fraud Examiners, 1–106.*

ii. *Almasria, N. A. (2022). Corporate governance and the quality of audit process: An exploratory analysis considering internal audit, audit committee and board of directors. European Journal of Business and Management Research, 7(1), 78–99. https://doi.org/10.24018/ejbmr.2022.7.1.1210*

iii. *Bernardo, B. M. V., Mamede, H. S., Barroso, J. M. P., & dos Santos, V. M. P. D. (2024). Data governance & quality management—Innovation and breakthroughs across different fields. Journal of Innovation and Knowledge, 9(4). https://doi.org/10.1016/j.jik.2024.100598*

iv. *Bhasin, M. (2016). Contribution of forensic accounting to corporate governance: An exploratory study of an Asian country. SSRN Electronic Journal, 10(April), 479–492. https://doi.org/10.2139/ssrn.2676488*

v. *Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. Journal of Information Systems, 31(3), 5–21. https://doi.org/10.2308/isys-51804*

vi. *Familoni, B. T. (2024). Cybersecurity challenges in the age of AI: Theoretical approaches and practical solutions. Computer Science & IT Research Journal. 5, 703-724. https://doi.org/10.51594/csitrj.v5i3.930*

vii. *Haddad, H., Alharasis, E. E., Fraij, J., & Al-Ramahi, N. M. (2024). How do innovative improvements in forensic accounting and its related technologies sweeten fraud investigation and prevention? WSEAS Transactions on Business and Economics, 21, 1115–1141. https://doi.org/10.37394/23207.2024.21.93*

viii. *Kaawaase, T. K., Nairuba, C., Akankunda, B., & Bananuka, J. (2021). Corporate governance, internal audit quality and financial reporting quality of financial institutions. IAsian Journal of Accounting Research, 6(3), 348–366. https://doi.org/10.1108/AJAR-11-2020-0117*

ix. *Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. Journal of Emerging Technologies in Accounting, 14(1), 115–122. https://doi.org/10.2308/jeta-51730*

x. *Malik, A. W., Bhatti, D. S., Park, T.-J., Ishtiaq, H. U., Ryou, J.-C., & Ki-II Kim. (2024). Cloud digital forensics: Beyond tools, technique, and challenges. Sensors, 24, 433, 1–30. https://doi.org/10.3390/s24020433*

xi. *Oluwatosin Ilori, Nelly Tochi Nwosu, & Henry Nwapali Ndidi Naiho. (2024). Advanced data analytics in internal audits: A conceptual framework for comprehensive risk assessment and fraud detection. Finance & Accounting Research Journal, 6(6), 931–952. https://doi.org/10.51594/farj.v6i6.1213*

xii. *Rezaee, Z., & Riley, R. (2022). Financial statement fraud: Prevention and detection (2nd ed.). Wiley. https://doi.org/10.4324/9781003200383-17*

xiii. *Singleton, T. W., & Singleton, A. J. (2010). Fraud auditing and forensic accounting. 4th ed. pp. 1-313. Wiley, John Wiley & Sons, Inc.*