

Data analytics and internal controls in U.S. financial systems: A review of fraud detection and financial reporting integrity

Francesca Nyarkoa Kobla ^{1,*} and Jessica Fosua Agyei ²

¹ Harbert College of Business, Business Analytics and Information Systems, Auburn University, AL USA.

² School of Business, University of Capecoast, Ghana.

Magna Scientia Advanced Biology and Pharmacy, 2026, 18(02), 082–095

Publication history: Received on 20 June 2026; revised on 27 July 2026; accepted on 30 July 2026

Article DOI: <https://doi.org/10.30574/msabp.2026.18.2.0060>

Abstract

This integrative review explores the role of data analytics and internal control systems in preventing fraud and financial reporting integrity in financial systems in the United States. The study adopts an integrative literature review approach that brings together a body of peer-reviewed research, regulatory publications, audit research, and financial technology literature to examine the use of analytics to detect fraud, the role of internal control over financial reporting, continuous monitoring, and emerging financial oversight technologies in an evolving regulatory and governance landscape. The results suggest that data analytics plays a crucial role in improving transaction surveillance, anomaly detection, risk assessment, and continuous auditing, especially when coupled with machine learning and AI monitoring tools. But the effectiveness of these technologies is still impacted by data quality challenges, model risk, implementation differences, explainability concerns and governance constraints. The review also continues to highlight the role of internal controls to ensure accountability, oversight and reliable reporting processes to support the effective utilization of analytical outputs in financial assurance environments. The study concludes that strengthening fraud detection and financial reporting integrity requires integrating analytics and internal controls within a unified governance framework supported by continuous monitoring, institutional accountability, and transparent oversight mechanisms.

Keywords: Data Analytics; Fraud Detection; Internal Controls; Continuous Auditing; Financial Reporting

1. Introduction

The U.S. financial system is one of the most technologically advanced and institutionally regulated financial systems in the world. For some time now, digital banking infrastructure, algorithmic trading systems, cloud-based financial platforms, and real-time payment technologies have revolutionized the way financial information is created, processed, monitored, and reported. Financial institutions now have to deal with massive amounts of transactional data in highly intertwined systems that run continuously and at high speed. These advances, which have enhanced the efficiencies, scalability, and market access, have also heightened the risk of exposure to complex financial fraud and reporting manipulation (Udeh et al., 2024). In the past, fraud detection within financial institutions was largely dependent on manual oversight, periodic audits, rule-based monitoring systems, and retrospective investigations (Westland, 2020; Celestin, 2020). While these measures laid an initial groundwork of protections, they were developed for more stable and less complicated financial markets. Conventional audit methods were mostly based on sampling of transactions and review cycles that were not performed in real time, making it difficult for the institutions to detect suspicious transactions (Ding, 2023). However, with the growing volume of transactions and the increasing digitization of financial operations, these traditional approaches were unable to keep up with the speed and volume of today's financial systems (Oguntibeju et al., 2024).

* Corresponding author: Francesca Nyarkoa Kobla

Data analytics has revolutionized the world of fraud detection and financial monitoring. Today, financial institutions use predictive analytics, machine learning models, anomaly detection, and automated monitoring systems to detect unusual transaction data, analyze behavioral risks, and enhance their monitoring capabilities (Ali et al., 2022; Gkegkas et al., 2025). Unlike traditional systems, analytics-based systems can process large amounts of information on a continuous basis, allowing institutions to detect abnormal activities earlier and be more responsive to potential fraud (Abikoye et al., 2024). This trend towards data-driven financial oversight has been further propelled by the increasing role of AI in compliance, auditing, and risk management operations (Amoako et al., 2025; Tiwari, 2023). In parallel, internal controls continue to play a key role in the integrity and reliability of financial reporting in financial institutions in the United States (Rashid, 2022; Krishnan et al., 2020). The enactment of the Sarbanes-Oxley Act of 2002, following financial disclosure scandals prevalent in the corporate world, made internal control systems more relevant in protecting financial disclosures and maintaining investor confidence (Liu & Huang, 2020). The expectations for accountability of governance, the quality of audit reporting, transparency, and Internal Control over Financial Reporting (ICFR) have been influenced by ongoing oversight by institutions such as the Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB) (Aobdia et al., 2025; Weickgenannt et al., 2021). The frameworks mandate organizations to put in place control mechanisms that enable the prevention of unauthorized activities, identification of reporting irregularities, and the accuracy of financial statements (Adeboye et al., 2021; Mohammed et al., 2021).

Notwithstanding these developments, fraud detection and financial reporting integrity remain significant challenges in the U.S. financial system. Financial fraud is no longer just about the manipulation of accounting figures, but an ecosystem involving transactional fraud, cyber-enabled financial crimes, synthetic identity schemes, insider fraud, and digitally coordinated financial crime (Sánchez-Aguayo et al., 2021; Homer, 2020). Institutional risk exposures have grown in scale and complexity as a result of the growing integration of financial technologies, automated reporting systems, and cloud-based infrastructure. Fraudulent activities can now occur across multiple systems simultaneously, often making detection more difficult and increasing the potential for operational and reputational damage.

A recurring issue is that fraud detection systems are still not very effective, even after significant investment in technology. There are still many analytics-driven monitoring solutions that generate high numbers of false-positive alerts, which puts strain on compliance operations and diminishes investigative effectiveness (Oguntibeju et al., 2024; Gkegkas et al., 2025). The ability of institutions to identify suspicious activity from legitimate transactions is challenged in certain environments because of similar behaviors and the changing nature of fraud techniques. Machine learning systems trained on past fraud data may also have a poor ability to detect fraud schemes that are not observed in the past. Fraud schemes are becoming increasingly adaptable, and detection methods need to continuously improve to be effective.

In today's increasingly automated financial landscape, internal control systems are under increasing pressure as well. Many institutions have formally established control frameworks, but there is some variability in how well the frameworks are implemented in operational settings (Gupta et al., 2025). Configuration changes, excessive user privileges, and lax oversight mechanisms can allow automated controls within enterprise systems to be circumvented (Rashid, 2022). Coordinating between departments in charge of compliance, auditing, cyber security, and financial reporting can be a challenge in highly interdependent environments if control structures are fragmented (Kaawaase et al., 2021). Incorporating financial operations into a cloud-based infrastructure and outsourced service environments has made institutional accountability and institutional control monitoring even more complex. The rapid growth of financial data has also put a strain on the effectiveness of traditional audit methodologies. Traditional periodic review systems are now not capable of handling the volume of financial institutions' transactions (Zhou, 2020). Consequently, there have been concerns about the effectiveness of sample-based auditing in settings where financial transactions occur regularly and frequently (Mudawanah et al., 2024). There has been a focus on continuous auditing and real-time monitoring frameworks as potential solutions, but adoption can be challenging and costly in terms of technology, governance, and organizational change (Minkkinen et al., 2022).

With the growing use of artificial intelligence in financial decision-making, there have also been emerging concerns. Risks related to model opacity, model explainability, and accountability may arise from AI-driven applications in fields like credit assessment, fraud monitoring, investment analysis, and algorithmic trading (Svetlova, 2022; Pallapati & Oman-Amoako, 2026). Sometimes the outputs of complex machine learning systems are not easily understood within existing governance mechanisms by auditors, regulators, and compliance practitioners (Sodnomdavaa & Lkhagvadorj, 2025). These concerns have sparked further discussion on the need for explainable AI, ethical regulation, and the potential long-term reliability of automated financial governance systems (Owolabi et al., 2024).

In view of these changes, data analytics and internal controls have become a growing part of the discussion on fraud prevention and the integrity of financial reporting. Financial institutions are not working in an environment where technology and governance have no interdependency. Rather, the ability to leverage analytics-driven monitoring capabilities to effectively detect fraud is increasingly reliant on the integration of these tools into institutional control systems, audit frameworks, compliance programs, and reporting processes (Amoako et al., 2026; Ampofo & Amoakoh, 2026). The understanding of this interaction is increasingly crucial in supporting financial oversight and maintaining confidence in financial reporting systems within the United States.

This integrative research study seeks to explore how data analytics and internal control systems contribute to fraud detection and financial reporting integrity in the U.S. financial systems. This review draws on conceptual, empirical, regulatory, and institutional literature and examines the roles of analytics technologies and control frameworks in financial oversight, financial reporting reliability, and fraud risk management. It also explores emerging technologies, operational constraints, governance issues, and changing institutional practices that will impact the future of fraud detection and reporting integrity within the U.S. financial system.

2. Conceptual and Theoretical Foundations

In the context of financial systems, data analytics involves applying computational, statistical, and AI-driven methods to analyze financial data to identify anomalies, patterns, and risk indicators (Westland, 2020; Tiwari, 2023). In fraud detection and reporting monitoring, analytics enables transaction monitoring, behavioural monitoring, anomaly detection, and continuous monitoring (Ali et al., 2022; Oguntibeju et al., 2024). Predictive and machine learning models are becoming popular tools to detect and flag unusual financial activities that could signal fraud, control failure, or reporting irregularity (Amoako et al., 2025; Gkegkas et al., 2025). Compared to conventional sampling methods, analytics systems can analyze vast numbers of transactions in near real-time, enhancing the speed and scale of financial surveillance (Abikoye et al., 2024; Zhou, 2020). The effectiveness of the analytics, however, relies on data quality, the reliability of the models, and the ability to interpret and act on the analytical output in an appropriate way (Bower et al., 2024; Sodnomdavaa & Lkhagvadorj, 2025).

Internal controls are the system of controls that support the integrity of financial reporting. They include policies, procedures, and system-based mechanisms that are implemented to ensure that financial information is accurate, reliable, and meets reporting requirements (Mohammed et al., 2021; Rashid, 2022). The COSO framework continues to be the predominant tool that guides internal control processes within U.S. financial institutions and focuses on the control environment, risk assessment, control activities, communication, and monitoring (Adeboye et al., 2021; AL-dalmi & Qader, 2021). Internal Control over Financial Reporting (ICFR) is a key component of financial reporting that helps achieve disclosure accuracy, accountability, and audit reliability (Krishnan et al., 2020; Weickgenannt et al., 2021). Key controls involve segregation of duties, authorization, reconciliation, audit trails, and IT general controls for system access and change management (Gupta et al., 2025; Liu & Huang, 2020).

In today's financial systems, fraud detection is no longer limited to identifying financial statement manipulation but also covers transactional fraud, asset misappropriation, anti-money laundering offences, insider fraud, and digitally-enabled financial crimes (Malysheva, 2020; Udeh et al., 2024). Traditional detection methods were based on manual analysis and pre-defined rules, which tended to restrict detection capability in complex financial situations (Celestin, 2020). Today, analytics-based detection systems employ anomaly detection, behavioural profiling, and risk-scoring to detect suspicious activity proactively (Ampofo & Amoakoh, 2026; Amoako et al., 2025). However, fraud is adaptable, and systems need to continually evolve with the changing fraud tactics and operational risk (Sánchez-Aguayo et al., 2021; Homer, 2020).

Financial reporting integrity indicates the faithful representation of an institution's financial position and operations in the reported financial information (Ding, 2023). Reporting integrity is not only determined by adherence to accounting principles, but also by the effectiveness of governance mechanisms, internal controls, and audit systems, which underpin financial disclosure systems (Kaawaase et al., 2021; Emeza & Brakye, 2025). The Fraud Triangle Theory, Agency Theory, and COSO Internal Control Framework are the main theories that underpin this review. According to Fraud Triangle Theory, fraud is an interaction between pressure, opportunity, and rationalisation (Homer, 2020; Sánchez-Aguayo et al., 2021), and Agency Theory emphasises the conflicts of interest between managers and stakeholders, which can lead to financial misrepresentation. The COSO framework establishes the framework in which institutions build and assess their internal controls to help lower fraud risk and increase the reliability of reporting (Mohammed et al., 2021; Gupta et al., 2025). These viewpoints together illustrate how the advancement of technology does not completely eradicate the risk of fraud without proper governance, accountability, and control enforcement (Svetlova, 2022; Pallapati & Oman-Amoako, 2026).

3. Methodology

This study utilizes an integrative review method since the topic is multifaceted, having elements that fall under accounting, auditing, financial governance, information systems, fraud analytics, and regulatory oversight. The integrative approach can be used if a topic is not based on one methodological tradition, but on empirical studies, conceptual research, guidance by regulations and practitioner publications. Additionally, regulatory and professional publications from various industry regulatory bodies, including the Securities & Exchange Commission (SEC), the Public Company Accounting Oversight Board (PCAOB), the Committee of Sponsoring the Treadway Commission (COSO), the Financial Crimes Enforcement Network (FinCEN), and the Association of Certified Fraud Examiners (ACFE), were reviewed due to their relevance to governance frameworks, compliance expectations, and fraud oversight practices in the U.S. financial environment.

Literature search was performed in selected academic databases and scientific search engines like Google Scholar, Scopus, ScienceDirect, and ResearchGate. The relevant regulatory and institutional documents were also retrieved from official publications and reports of SEC, PCAOB, COSO and FinCEN. The literature search covered the period from 2020 to 2026 to reflect the latest advances in financial analysis, fraud detection, internal controls, AI-based controls and financial reporting governance.

The search process utilized combinations of keywords and search phrases including “data analytics in fraud detection,” “internal controls and financial reporting,” “continuous auditing,” “AI in financial oversight,” “machine learning fraud detection,” “financial reporting integrity,” “real-time monitoring systems,” “RegTech,” “continuous monitoring,” and “explainable AI in finance.” Thirty-six sources were subjected to a review, which included peer-reviewed journal articles, conference papers, dissertations, regulatory publications, accounting and audit studies, financial technology research, and other scholarly sources pertinent to fraud detection in financial systems and financial reporting integrity. Materials that were not directly related to the focus of the study were excluded, such as duplicate studies, non-English publications, studies which did not discuss financial systems, or materials which were insufficiently relevant to the concepts of fraud analytics, internal controls, or financial oversight. The selection process focused studies that directly related to fraud detection technologies, internal control frameworks, governance mechanisms, audit analytics, continuous monitoring systems and financial reporting reliability in financial institutions.

The study objectives, analytical methods, control mechanisms, institutional findings, governance implications, and technological limitations mentioned in the literature were the major concerns of data extraction process. This selected literature was subsequently synthesized thematically for patterns, trends, governance issues, operational issues, and institutional issues in relation to data analytics and internal controls in fraud detection and financial reporting.

4. Data Analytics in Fraud Detection Systems

4.1. Evolution of Analytics-Driven Fraud Detection

Financial institutions have developed their fraud detection systems from rule-based monitoring to advanced analytical models (Westland, 2020; Celestin, 2020). Early detection systems focused mainly on predefined rules, fixed thresholds, and exception reporting to recognize suspicious transactions. These methods worked well for spotting the obvious irregularities, but they were ineffective in detecting complex or adaptive fraud schemes, which resulted in many false-positive alerts (Ali et al., 2022; Oguntibeju et al., 2024). As financial institutions accumulated larger transaction datasets and computing capabilities improved, statistical and predictive analytics became more widely integrated into fraud monitoring processes (Udeh et al., 2024; Tiwari, 2023). These methods allowed institutions to discover relationships and transaction patterns that were not apparent in a manual review or fixed rule structure. Eventually, machine learning models, anomaly detection systems, and behavioral analytics further broadened detection capabilities, enabling systems to detect unusual activities by learning from and adapting to changes in transaction patterns, rather than relying on preconceived notions (Amoako et al., 2025; Gkegkas et al., 2025).

The present phase of fraud identification is marked by the real-time tracking of transactions and AI-driven surveillance systems that can handle significant volumes of transactions over many interrelated financial platforms at any given moment (Abikoye et al., 2024; Malysheva, 2020). Such systems integrate various analytical methods, such as predictive modeling, behavioural profiling, and network analysis, to boost detection responsiveness and enhance coverage throughout the financial operations (Ampofo & Amoakoh, 2026; Ali et al., 2022). But with the advancement of these fraud detection systems, there are also growing concerns over model reliability, data governance, model explainability, and control oversight (Sodnomdavaa & Lkhagvadorj, 2025; Svetlova, 2022). The effectiveness of analytics-driven fraud

detection is increasingly reliant on governance and control frameworks around analytics systems as well as analytical capabilities (Pallapati & Oman-Amoako, 2026; Owolabi et al., 2024).

4.2. Machine Learning and Predictive Fraud Detection

In financial institutions, machine learning has emerged as a crucial aspect of fraud detection systems (Ali et al., 2022; Tiwari, 2023). Suspicious transaction patterns, behavioral irregularities, and high-risk activities are increasingly being detected using machine learning systems like decision trees, random forests, neural networks, convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory (LSTM) models (Amoako et al., 2025; Gkegkas et al., 2025). The scalability and deployment of predictive fraud detection models within financial high-volume settings have also been enhanced with the evolution of GPU computing and automated machine learning (AutoML) platforms (Oguntibeju et al., 2024). Machine learning models can process a vast amount of data and detect correlations between variables that might not be apparent in manual processes (Udeh et al., 2024; Westland, 2020).

In high-volume financial settings, predictive fraud detection systems are especially appreciated for their scalability, automation, and precision in fraud detection (Ampofo & Amoakoh, 2026; Abikoye et al., 2024). These systems can prioritize transaction risks, detect abnormal transaction patterns, and assist in real-time monitoring on payment platforms, digital banking systems, and anti-money laundering processes (Malysheva, 2020; Amoako et al., 2025). While these benefits exist, machine learning systems come with critical governance and reliability issues as well. The quality, representativeness, and stability of training data are crucial for predictive models, as biased or incomplete data can impact detection results and introduce risks of false positives (Bower et al., 2024; Ali et al., 2022). In addition, some advanced models operate with limited explainability, making it difficult for auditors, regulators, and compliance personnel to understand how specific decisions or risk scores were generated (Sodnomdavaa & Lkhagvadorj, 2025; Svetlova, 2022). This is why predictive analytics systems are typically more effective when used as decision support tools than as automated decision makers (Owolabi et al., 2024; Pallapati & Oman-Amoako, 2026). Human oversight is very important, especially in cases of fraud investigation, financial reporting, and regulatory disclosure (Yeboah et al., 2026; Amoakoh et al., 2026).

4.3. Real-Time Monitoring and Continuous Auditing

Real-time monitoring and continuous auditing have revolutionized the way financial institutions detect fraud and supervise financial activities (Abikoye et al., 2024; Zhou, 2020). Real-time transaction monitoring systems assess transactions in real-time and flag suspicious activity before a transaction is completed, not after it has caused financial harm (Malysheva, 2020; Oguntibeju et al., 2024). These systems are commonly employed in payment systems, digital banking, and anti-money laundering (AML) processes, where swift detection is essential (Udeh et al., 2024; Amoako et al., 2025).

Continuous auditing adds this functionality to audit and control environments by using a larger number of transactions to conduct analytical procedures in a continuous manner, not just periodically (Mudawanah et al., 2024; Zhou, 2020). Continuous monitoring systems also enable continuous evaluation of control performance, exception activity, and operational irregularities in financial systems (Minkinen et al., 2022; Álvarez-Foronda et al., 2023). These measures provide added security when taken together because they help to minimize the chances of control weaknesses or fraud patterns going undetected for long periods (Celestin, 2020; Ding, 2023).

Modern fraud monitoring systems have also increasingly been dependent on dashboard-based monitoring platforms. These interfaces enable compliance personnel, auditors, and risk managers to view alerts, exception trends, risk scores, and transaction anomalies in real time in a centralized environment (Ampofo & Amoakoh, 2026; Amoakoh et al., 2026). But, the level of effectiveness of real-time monitoring should rely not just on technological capability, but also on the institutional responsiveness. High alert volumes, unclear escalation procedures, weak follow-up processes, and analyst fatigue can reduce the practical effectiveness of monitoring systems even when analytical models are technically advanced (Bower et al., 2024; Pallapati & Oman-Amoako, 2026).

4.4. Data Quality and Fraud Detection Reliability

The quality and integrity of the data in monitoring systems are fundamental to the reliability of analytics-based fraud detection (Bower et al., 2024; Udeh et al., 2024). Data quality issues like incomplete datasets, inconsistent reporting formats, inaccurate records, and poor data governance can hinder detection capabilities and result in gaps within fraud surveillance procedures (Gkegkas et al., 2025; Celestin, 2020). Data environments that are poorly managed may give rise to unreliable outputs, even for advanced analytical models (Ali et al., 2022; Westland, 2020).

One of the most significant challenges in fraud detection systems is false-positive alerts (Oguntibeju et al., 2024; Abikoye et al., 2024). High alert levels can distract compliance staff, raise investigation expenses, and lead to analyst fatigue, all of which could result in a failure to timely identify or investigate real suspicious activities (Ampofo & Amoakoh, 2026; Malysheva, 2020). Meanwhile, due to incomplete or inadequately structured datasets, important fraud patterns can be missed and lead to detection blind spots in financial systems (Amoako et al., 2025; Udeh et al., 2024).

The reliability and fairness of predictive fraud models are also influenced by training data quality (Sodnomdavaa & Lkhagvadorj, 2025; Tiwari, 2023). Machine learning systems that are built from biased or unbalanced historical data can perpetuate skewed risk patterns or may flag some customer activities or transactions as suspicious (Owolabi et al., 2024; Svetlova, 2022). With the implementation of AI-based monitoring systems in financial institutions, regulatory issues related to transparency, fairness, and accountability of models have also grown (Pallapati & Oman-Amoako, 2026; Yeboah et al., 2026).

Data reliability challenges also emerge during data extraction, transformation, and integration processes. Financial institutions frequently integrate data from several sources, such as payment systems, customer databases, and enterprise reporting systems, which poses the risk of data mapping errors, incomplete integration, and inconsistencies in formatting (Álvarez-Foronda et al., 2023; Zhou, 2020). Therefore, the ability to detect fraud effectively relies not just on the analytical sophistication but also on a robust data governance framework, validated reporting processes, and reliable data management practices (Mohammed et al., 2021; Kaawaase et al., 2021).

4.5. Emerging Technologies in Fraud Detection

The financial landscape, particularly the mechanisms of fraud detection and financial oversight, keeps changing in the United States due to emerging technologies (Amoako et al., 2025; Gkegkas et al., 2025). Artificial intelligence, blockchain, natural language processing (NLP), robotic process automation (RPA), and intelligent compliance systems are being increasingly adopted in fraud monitoring and reporting to enhance analytical coverage, automation, and detection responsiveness (Tiwari, 2023; Udeh et al., 2024). For instance, blockchain is gaining popularity for its capacity to create an immutable record of transactions and improve the traceability in financial processes; meanwhile, NLP tools are now being utilized to examine unstructured data sources like financial disclosures, communications, and regulatory filings for inconsistencies or risk signals (Celestin, 2020; Ali et al., 2022).

RPA and intelligent automation systems have also helped to broaden the scope of repetitive monitoring and control tasks such as reconciliation processes, exception reporting, and compliance documentation (Emefa & Brakye, 2025; Abikoye et al., 2024). Meanwhile, the importance of explainable artificial intelligence (XAI) has surged in the context of fraud detection systems, driven by emerging regulatory and governance issues related to model transparency and accountability (Sodnomdavaa & Lkhagvadorj, 2025; Pallapati & Oman-Amoako, 2026). The interpretability of complex analytical models is increasingly enhanced by techniques such as SHapley Additive exPlanations (SHAP) and Local Interpretable Model-Agnostic Explanations (LIME), which can be used to guide regulatory review, auditability, and institutional oversight (Yeboah et al., 2026; Svetlova, 2022).

While emerging technologies have further broadened the analytical capabilities of fraud detection systems, their true impact will rely on the extent to which they increase the reliability of reports, control accuracy, and governance accountability in practice (Amoakoh et al., 2026; Ampofo & Amoakoh, 2026). Regardless of how technically savvy a technology is, if it cannot be properly explained, monitored, or controlled, then it presents new operational and compliance risks (Owolabi et al., 2024; Minkinen et al., 2022).

5. Internal Controls and Financial Reporting Integrity

5.1. Internal Control Systems in U.S. Financial Systems

Internal control systems in U.S. financial institutions are based on the COSO framework, which divides internal controls into the control environment, risk assessment, control activities, information and communication, and monitoring (AL-dalmi & Qader, 2021; Mohammed et al., 2021). These elements contribute to the accountability for operations, compliance with regulations, and financial reporting reliability (Adeboye et al., 2021; Gupta et al., 2025). Internal controls vary from institution to institution based on size, operations, and technology, but the goal is always the same, which is to minimize the risk of material misstatement, failure in operations, and unauthorized transactions (Krishnan et al., 2020; Liu & Huang, 2020).

The control environment sets the tone for the ethics, accountability, governance, and oversight within the institution and influences the effectiveness of other control mechanisms in practice (Weickgenannt et al., 2021; Kaawaase et al., 2021). Risk assessment processes are used to discover vulnerabilities that could impact reporting integrity or operational stability, and control activities involve specific responses in the form of authorization procedures, segregation of duties, controls for reconciling, approval workflows, and restriction of system access (Rashid, 2022). Monitoring functions are then used to determine if these controls are still effective in changing financial and technological environments (Mohammed et al., 2021; Gupta et al., 2025).

In many financial institutions, automated analytics, ongoing monitoring systems, and dashboard-type oversight tools are also assisting the monitoring and risk assessment processes, enabling institutions to detect control weaknesses earlier and respond to new risks in a timely fashion (Álvarez-Foronda et al., 2023; Zhou, 2020). But internal controls are only effective when they are functioning within a broader governance framework and not as standalone compliance processes (Ding, 2023). Reporting reliability throughout the financial system can be compromised due to weaknesses in a component of the control environment, especially in operational systems that are highly interconnected and data-intensive (Weickgenannt et al., 2021).

5.2. Internal Controls and Fraud Prevention

Internal controls have a significant role to play in preventing fraud, as they limit the opportunity for fraudulent activities to occur and increase institutional accountability (Rashid, 2022; Adeboye et al., 2021). Preventive controls aim to minimize the risk of misconduct by incorporating elements like access control, segregation of duties, authorization needs, and approval protocols (AL-dalmi & Qader, 2021; Mohammed et al., 2021). Detective controls help detect fraud by tracking unusual activity, reviewing exceptions to transactions, and analyzing unusual system activity, while corrective controls mitigate the detected weaknesses by implementing remediation actions or making adjustments to controls and responding to incidents as needed.

Automated controls have grown in significance in today's financial systems because they enable financial institutions to implement policies in a more consistent manner in large transaction environments (Abikoye et al., 2024; Zhou, 2020). Automated tools such as system-based approvals, access management systems, automated reconciliations, and continuous monitoring can help minimize reliance on manual controls, which in turn can help to create greater operational consistency (Álvarez-Foronda et al., 2023; Emefa & Brakye, 2025). The effectiveness of automated controls, however, is limited unless they are set up correctly, tested regularly, and backed by continuous monitoring activities (Minkinen et al., 2022; Amoakoh et al., 2026).

Governance accountability and organizational oversight are also crucial for fraud prevention (Kaawaase et al., 2021; Weickgenannt et al., 2021). The chances of identifying suspicious activities early enough to prevent larger reporting or operational failures are increased through whistleblower mechanisms, ethics reporting channels, and through the use of internal investigation procedures (Homer, 2020; Sánchez-Aguayo et al., 2021). Concurrently, management override is a major control risk in financial institutions, as those who control high authority and system access can override otherwise effective controls (Krishnan et al., 2020; Rashid, 2022). Consequently, many fraud prevention initiatives are now based on the concept of continuous monitoring and access reviews, as well as audit oversight to detect unusual activity by privileged users or unauthorized system changes (Mudawanah et al., 2024; Yeboah et al., 2026).

5.3. Internal Controls and Reporting Accuracy

Internal controls have a significant impact on the accuracy of financial reporting, as they minimize errors, enhance financial reconciliation processes, and increase the consistency of financial disclosures (Krishnan et al., 2020; Gupta et al., 2025). Institutions that have strong Internal Control over Financial Reporting (ICFR) are more likely to detect reporting irregularities in time to prevent them from becoming apparent in financial statements (Liu & Huang, 2020; Weickgenannt et al., 2021). However, material weaknesses in internal controls have often been linked with reporting restatements, diminished earnings quality, and diminished confidence in financial disclosures and reporting (Krishnan et al., 2020; Aobdia et al., 2025).

Automated control systems have also further enhanced the accuracy of reporting, with better validation and reconciliation of financial operations (Emefa & Brakye, 2025; Zhou, 2020). Automated reconciliations, system-imposed validation rules, variance analysis processes, and exception reporting features assist institutions in quickly detecting discrepancies and decreasing the potential for reporting errors to go unreported (Celestin, 2020; Álvarez-Foronda et al., 2023). These controls also help to enhance the reliability of the audit, as they allow for the generation of evidence trails that can be used for internal audit reviews and external audit procedures (Ding, 2023; Westland, 2020).

The effectiveness of reporting controls is not only related to their existence, but also to the accuracy and consistency of their operation (Mohammed et al., 2021; Rashid, 2022). The poorly designed, weakly enforced, or inadequately monitored controls can be ineffective in detecting material reporting problems despite the existence of formal compliance controls (Adeboye et al., 2021; AL-dalmi & Qader, 2021). Accordingly, the extent to which financial reporting is accurate relies significantly on the overall quality of governance, oversight, and control in financial institutions (Kaawaase et al., 2021).

There are also institutional and market implications of reliable financial reporting. Credible disclosures build investor confidence, contribute to regulatory trust, and enhance the credibility of the financial markets, whereas issues with the integrity of disclosures can harm institutional reputation and erode confidence in financial oversight institutions (Ding, 2023; Gupta et al., 2025).

5.4. Technology-Enabled Internal Controls and Regulatory Reporting Governance

Technology-enabled controls are increasingly transforming internal control and reporting governance processes within U.S. financial institutions (Álvarez-Foronda et al., 2023; Zhou, 2020). Automated reconciliation platforms, like BlackLine and Trintech, enable organizations to automate their reconciliation, exception management, and financial close processes and create audit trails for the monitoring of management and external audits (Emefa & Brakye, 2025; Celestin, 2020). AI-based control testing and smart audit systems have also helped institutions to test and audit larger numbers of transactions, access logs, approvals, and control activities more continuously, rather than using a traditional sampling approach (Amoakoh et al., 2026; Yeboah et al., 2026).

In addition, tools such as robotic process automation (RPA), continuous compliance monitoring systems, and AI-powered audit platforms are also increasingly becoming part of governance and reporting frameworks to enhance monitoring agility, streamline repetitive compliance tasks, and bolster oversight of financial processes (Abikoye et al., 2024; Mudawanah et al., 2024). The systems provide real-time compliance monitoring, exception reporting, and risk tracking, enabling institutions to have more up-to-date information about their control environments and regulatory exposure (Ampofo & Amoakoh, 2026; Oguntibeju et al., 2024).

With this, the regulatory burden on documentation, oversight, and accountability has risen with the increasing digitization of financial reporting processes (Aobdia et al., 2025; Ding, 2023). Auditable and well-governed control environments are reinforced by the requirements of SOX, the reporting requirements of the SEC, the auditing standards of the PCAOB, and the model auditing guidance provided by banking regulators. Regulatory requirements are increasingly focusing on technologies that impact financial reporting and control evidence as governance and compliance matters, instead of just operational matters (Gupta et al., 2025; Weickgenannt et al., 2021).

The effectiveness of technology-based controls, therefore, relies not only on the automation functionality but also on the level of institutional oversight around these controls (Minkinen et al., 2022; Pallapati & Oman-Amoako, 2026). Poorly controlled, inadequately monitored, and weakly documented automated controls can decrease transparency instead of enhancing reporting integrity. Accordingly, financial institutions will need to make it explainable, auditable, and have clear escalation procedures, evidence standards, and human review in place to maintain technology-driven control environments (Sodnomdavaa & Lkhagvadorj, 2025; Amoako et al., 2025).

6. Intersection of Data Analytics and Internal Controls

6.1. Analytics and Internal Control Integration

Incorporating data analytics into internal control processes has drastically altered the way financial institutions confront fraud risk and internal control programs (Gkegkas et al., 2025; Celestin, 2020). Analytics-driven control environments enhance monitoring visibility, bolster control accuracy, and decrease time lags between irregular activity and institutional response (Abikoye et al., 2024; Zhou, 2020). Rather than static control procedures, organizations are increasingly turning to analytics to help them highlight transaction patterns, behavioural anomalies, and risk concentrations across their large and complex data populations, ensuring control systems are more targeted and responsive (Udeh et al., 2024; Oguntibeju et al., 2024).

Enterprise fraud management systems further extend this integration by combining transaction monitoring, behavioral analytics, risk scoring models, case management tools, and regulatory reporting functions within unified platforms (Amoako et al., 2025; Ampofo & Amoakoh, 2026). These systems usually include several different data signals such as transaction behavior, customer patterns and activity, account features, and external verification data, which help

provide a more thorough analysis of fraud risk (Ali et al., 2022; Tiwari, 2023). Hybrid control architectures that combine rule-based controls with machine learning models have become particularly common because they balance predictive capability with auditability and regulatory explainability (Sodnomdavaa & Lkhagvadorj, 2025; Pallapati & Oman-Amoako, 2026).

The effectiveness of such systems is to a great extent reliant on the integration of the analytics and internal control within wider governance frameworks. While analytics can enhance fraud visibility and risk identification, internal controls can dictate how institutions react to identified risks by way of escalation, approval controls, monitoring, and remediation efforts (Rashid, 2022; Adeboye et al., 2021). The governance of analytical models, data, alert systems, and risk-scoring workflows that impact fraud detection and reporting decisions has also been introduced as part of the control environment, which is expanding beyond procedural oversight (Minkinen et al., 2022; Owolabi et al., 2024).

6.2. Continuous Auditing and Continuous Monitoring

Continuous auditing and continuous monitoring have significantly changed how financial institutions approach assurance and oversight activities (Zhou, 2020; Mudawanah et al., 2024). These systems use automated analytical tools to assess transactions, controls, and reporting activities more often and, in some instances, almost in real time (Abikoye et al., 2024; Westland, 2020). This enhances the responsiveness of the oversight, quickens the process of detecting anomalies, and enables timely remediation of operational and reporting irregularities (Oguntibeju et al., 2024; Gkegkas et al., 2025). The incorporation of continuous auditing and monitoring systems has also helped to make auditing and compliance more adaptable. Institutions are increasingly employing automated audit platforms and analytics-based monitoring systems to achieve continuous visibility and monitoring of high-risk operational areas and control activities, and not just relying on periodic audit cycles (Amoakoh et al., 2026; Yeboah et al., 2026).

This enables audit and compliance resources to be more agile in responding to evolving risk circumstances and newly emerging fraud signals. These systems are especially useful in high-volume financial settings where periodic review systems might not be able to offer a sufficient level of oversight coverage (Abikoye et al., 2024; Westland, 2020). However, their effectiveness is highly dependent on the quality of governance, alert management structures, and institutional response capacity. Even though continuous monitoring systems may provide improved assurance, the operational costs and benefits of such systems can be compromised by high volumes of alerts, poor definition of escalation processes, and inadequate investigative resources (Rashid, 2022; Svetlova, 2022).

6.3. Institutional and Operational Challenges

Although analytics and internal controls are increasingly being used in financial institutions, the effectiveness of implementation is still hindered by institutional and operational challenges (Amoako et al., 2025; Gkegkas et al., 2025). One major challenge to implementation is high costs, especially for institutions with legacy systems and low technological infrastructure (Krishnan et al., 2020; Abikoye et al., 2024). There is a need for ongoing investment into technology, data management, cybersecurity, model governance and expert manpower to support advanced analytics platforms, continuous monitoring systems and AI based control environments (Ampofo & Amoakoh, 2026; Amoakoh et al., 2026).

In addition, as institutions become more centralized to store extensive amounts of financial and operational information in unified analytics spaces, cybersecurity and data governance threats also grow in complexity (Udeh et al., 2024; Bower et al., 2024). As a result of the growing capabilities of analytics platforms, there is also an increased risk of exposure to unauthorised access, manipulation of data, and fraud attempts to bypass fraud detection tools (Ali et al., 2022; Tiwari, 2023). Concurrently, financial institutions face increasing complexity in meeting regulatory demands relating to financial reporting, data governance, privacy obligations, Model risk management, and AI oversight demands (Aobdia et al., 2025; Gupta et al., 2025).

While implementing technology is part of the operational challenge, so too are other factors that impact its implementation and use (Minkinen et al., 2022; Pallapati & Oman-Amoako, 2026). Analytics-based systems of oversight can be undermined by issues of explainability of AI models, governance processes, employee resistance, and the reliability of the models themselves (Svetlova, 2022; Owolabi et al., 2024). However, as fraud patterns change over time, models may degrade in performance, especially if they are not exposed to conditions similar to those in the data used for their training (Sodnomdavaa & Lkhagvadorj, 2025). The increasing dependence on automated analytical outputs by institutions, also increases the expectations for documentation, accountability, escalation processes and human oversight (Weickgenannt et al., 2021; Rashid, 2022). The governance of AI and GenAI is now increasingly considered as internal control, not just a technical issue, as evidenced by the recent guidance provided by the regulators (Yeboah et al., 2026; Pallapati & Oman-Amoako, 2026).

6.4. AI Governance and Accountability in Financial Oversight

AI governance has become a critical institutional control issue in U.S. financial institutions as AI systems are increasingly being used in fraud detection, compliance monitoring, and financial reporting (Pallapati & Oman-Amoako, 2026; Yeboah et al., 2026). The governance frameworks of AI systems are becoming a major regulatory and institutional concern, particularly in the context of financial services, where AI systems are increasingly used to inform credit risk assessment, transaction monitoring, regulatory reporting and audit analytics (Sodnomdavaa & Lkhagvadorj, 2025; Owolabi et al., 2024).

One of the key challenges in AI governance is model explainability. Many sophisticated machine learning systems, such as deep neural networks and ensemble learning models, are not easily interpretable by auditors, regulators, or compliance personnel (Svetlova, 2022; Sodnomdavaa & Lkhagvadorj, 2025). AI models that produce fraud risk scores, flag suspicious transactions, or aid in the reporting process without providing clear reasoning can lead to gaps in accountability, potentially undermining institutional control objectives (Owolabi et al., 2024; Pallapati & Oman-Amoako, 2026). Model interpretability has been enhanced through techniques like SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-Agnostic Explanations), but their application in institutional oversight varies across the U.S. financial sector (Yeboah et al., 2026; Svetlova, 2022).

Algorithmic bias and fairness are also major governance issues of concern. AI systems that are trained on past financial data can inadvertently perpetuate patterns that disproportionately impact specific customer segments, geographic regions, or types of transactions, which can raise ethical and regulatory concerns (Owolabi et al., 2024; Pallapati & Oman-Amoako, 2026). U.S. financial regulators, such as the Securities and Exchange Commission (SEC) and the Office of the Comptroller of the Currency (OCC), have increasingly called for transparency, fairness, and accountability in AI-driven financial decision-making, especially when automated systems impact credit access, fraud investigations, or compliance reporting (Aobdia et al., 2025; Gupta et al., 2025). As such, financial institutions are expected not only to implement robust analytical systems but also to have governance frameworks that are auditable, explainable, and defensible in the face of regulatory examination.

In financial institutions, model risk management has emerged as a crucial aspect of AI governance (Yeboah et al., 2026; Amoakoh et al., 2026). Governance expectations are increasingly calling for institutions to have strong model validation procedures, such as back-testing, performance benchmarking, drift detection, and human review of automated outputs (Minkinen et al., 2022; Sodnomdavaa & Lkhagvadorj, 2025; Aobdia et al., 2025). Failure to implement these governance processes can lead to operational risk from suboptimal models and regulatory risk due to weak oversight of AI-driven control environments at institutions.

The advent of Generative AI (GenAI) has added further governance challenges. Large Language Models offer opportunities in the domain of compliance documentation, regulatory interpretation, and audit summarization, but they also pose risks due to issues with inaccurate outputs, synthetic data manipulation, and AI-powered fraud schemes (Pallapati & Oman-Amoako, 2026; Yeboah et al., 2026). In response, institutions are increasingly looking for formal review protocols, output validation procedures, and documentation standards that go beyond the existing paradigm of predictive model governance. AI governance frameworks in top U.S. financial institutions are thus moving towards a full lifecycle approach, integrated into a broader institutional control framework that includes model design, data source, deployment, monitoring, and retirement, rather than being confined to a one-off technical task (Amoakoh et al., 2026; Owolabi et al., 2024).

7. Discussion

The results of this review support the notion that data analytics and internal controls are transforming fraud detection and financial statement oversight for financial institutions in the United States (Amoako et al., 2025; Gkegkas et al., 2025). The literature also shows that the effectiveness of these advances is not just the sophistication of the analytical tools, but the level of institutional governance, control maturity, and regulatory accountability frameworks (Krishnan et al., 2020; Mohammed et al., 2021). This interaction not only affects institutional performance but also the overall stability, transparency, and credibility of U.S. capital markets.

A key takeaway from the literature is that improved internal controls and analytics-based oversight are important factors in building investor confidence and enhancing capital market efficiency. The institutions that have a credible disclosure process and have effective Internal Control over Financial Reporting (ICFR) minimize information asymmetry between the institutions and the market participants, which helps them to make informed investment and lending decisions (Ding, 2023; Gupta et al., 2025). Investors' trust in the financial information provided by firms has

been linked to strong control environments, which in turn have been correlated with higher earnings quality, lower disclosure risk, tighter credit spreads, and lower costs of capital (Krishnan et al., 2020; Liu & Huang, 2020). On the other side, material weaknesses in internal controls and reporting irregularities have been associated with reputation damage, loss of investors' confidence, and general market disruption, especially when material weaknesses are found in systemically important institutions (Weickgenannt et al., 2021; Aobdia et al., 2025).

These benefits are further enhanced by analytics-based monitoring, which ensures more reliable and timely financial monitoring procedures. Anomaly detection, exception management of controls, and real-time monitoring are features of continuous monitoring systems that help institutions detect and respond to control exceptions, preventing them from becoming material reporting issues or regulatory violations (Abikoye et al., 2024; Zhou, 2020). These features help in providing more accurate and consistent financial disclosures, valued by investors, regulators and ratings agencies evaluating institutional risk (Gupta et al., 2025; Weickgenannt et al., 2021). The quality of financial information flowing through U.S. capital markets could benefit from the increasing integration of analytics-control, which would help with more efficient price discovery, better risk assessment, and more systemic resilience.

One of the recurring themes in the literature is the conflict between the predictive analytical ability and the governance requirements to make these systems trustworthy (Sodnomdavaa & Lkhagvadorj, 2025; Pallapati & Oman-Amoako, 2026). While advanced fraud detection systems can significantly improve detection rates using deep learning, behavioral analytics, and real-time monitoring architectures, they also pose challenges in terms of explainability, auditability, and transparency in regulatory and compliance frameworks (Ali et al., 2022; Svetlova, 2022). This reflects an ongoing tradeoff between predictive accuracy and interpretability that explainable AI techniques have only partially resolved. The problem is particularly relevant in financial oversight, where regulators, investors, auditors, and compliance officers need to have confidence in the results of the analytical systems as well as the processes that lead to the production of those results (Owolabi et al., 2024; Yeboah et al., 2026).

There is also evidence in the literature that the most effective way for analytics and internal controls to function is as part of a unified governance framework, as opposed to as standalone functions (Rashid, 2022; Adeboye et al., 2021). Analytics increases visibility of anomalies, transaction patterns, and developing fraud signals, and internal controls offer governance processes to investigate alerts, address control gaps and ensure reliability of reporting (Zhou, 2020; Álvarez-Foronda et al., 2023). If there is a significant investment in analytical systems but not the same degree of governance and control, it is likely that the institutions will raise large numbers of alerts with insufficient institutional response capacity, thereby weakening the degree of operational effectiveness and reporting reliability. This integration gap has important implications for both regulatory confidence and market trust, as sophisticated analytical tools cannot independently guarantee credible financial oversight.

Another issue raised in the literature is the disparity in analytical and governance skills in the U.S. financial sector (Amoakoh et al., 2026; Amoakoh & Amoakoh, 2026). Advanced fraud analytics and continuous monitoring systems are usually more feasible for large financial institutions, which have the technological infrastructure, specialized expertise, and governance resources to support these systems. Smaller institutions, such as community banks, credit unions, and regional financial institutions, may be more likely to have issues with cost, staffing, legacy systems, and governance capacity (Krishnan et al., 2020; Gupta et al., 2025). This imbalance results in greater systemic weaknesses, as fraudsters can take advantage of less robust control environments, where monitoring and oversight are less effective (Udeh et al., 2024; Gkegkas et al., 2025).

The adaptive nature of financial fraud further intensifies these risks. AI-powered methods, synthetic identities, and orchestrated cyber-financial frauds that exploit existing fraud detection frameworks are becoming more common in fraud schemes (Amoako et al., 2025; Tiwari, 2023). Static fraud models and legacy detection frameworks become less effective as fraudulent methodologies evolve more rapidly than institutional responses. At the same time, the growing convergence of institutions around similar analytical architectures and machine learning models introduces the risk of correlated detection failures, where common weaknesses may be exploited across multiple institutions simultaneously (Sodnomdavaa & Lkhagvadorj, 2025; Amoakoh et al., 2026). This highlights the importance of ongoing model validation, institutional diversity in analytical design, and sustained regulatory oversight of AI governance frameworks as components of broader financial system stability.

In conclusion, the literature suggests that financial reporting integrity is not solely reliant on the technical accuracy of financial reporting but also on the credibility, transparency, and accountability of the institutional processes that underpin financial reporting (Ding, 2023; Kaawaase et al., 2021). The combination of well-governed analytical environments, effective internal controls, and auditable oversight mechanisms enhances the reliability of financial reporting and instills confidence in the financial market regarding financial institutions (Gupta et al., 2025;

Weickgenannt et al., 2021). Regulatory attention has therefore increasingly shifted toward the governance of analytical systems alongside their technical capabilities, reflecting the growing recognition that credible financial oversight requires both technological sophistication and accountable institutional governance structures (Aobdia et al., 2025; Yeboah et al., 2026).

8. Recommendation for U.S. Financial Institutions

The results of this review highlight some practical steps that could enhance fraud detection, financial reporting integrity, and governance accountability within U.S. financial institutions. Firstly, analytics should be embedded within unified governance and control structures. The most effective way to implement analytics-based fraud detection is within the context of a larger internal control and financial reporting system, not as a stand-alone technology department. Analytical models, alert management systems, escalation processes, and remediation processes should be part of the same governance framework to enhance institutional responsiveness, reporting accuracy, and audit preparedness. Implementation gaps between institutions should also be minimized. The financial sector is vulnerable to sophisticated fraud actors due to uneven analytical and governance capabilities. Collaborative intelligence-sharing frameworks, scalable RegTech solutions, and shared governance resources can support smaller and resource-limited institutions in enhancing their fraud detection and oversight processes and bolster the resilience of U.S. financial markets. Additionally, developing human oversight alongside automated systems is essential. Automated fraud detection and compliance systems still rely on good human judgment. Institutions should enhance training for audit, compliance, and risk management staff to better understand and interpret the analytical output, identify model limitations, and monitor the use of AI in decision-making processes. Continuous monitoring and auditing capabilities need to be expanded. Financial institutions should gradually shift from a traditional, periodic audit cycle to continuous monitoring of high-risk transactions and control activities. Institutions with limited infrastructure could enhance their monitoring capabilities and shorten the time between fraud and detection through phased technology investments, scalable Regulatory Technology (RegTech) solutions, and collaborative industry approaches. Also, there is a need to engage proactively with evolving regulatory expectations. Regulatory expectations surrounding AI governance, model risk management, and algorithmic accountability continue to evolve across the U.S. financial sector. Institutions should proactively follow SEC, OCC, Federal Reserve, PCAOB, and FinCEN guidance and ensure that new expectations are reflected in governance processes in advance of deficiencies becoming regulatory issues. Lastly, Financial institutions should prioritize AI governance as a formal control responsibility. Institutions need to establish comprehensive AI governance frameworks that include model validation, drift monitoring, explainability guidelines, bias evaluation, and human oversight to ensure that AI and machine learning systems are effective in preventing fraud, scoring risks, and complying with regulations. AI-driven outputs used in fraud investigations or regulatory reporting must remain transparent, interpretable, and defensible under regulatory scrutiny.

9. Conclusion

This integrative review focused on examining the relationship between data analytics, internal controls, fraud detection, and financial reporting integrity in the U.S. financial systems. The review highlights how analytics-driven tools can enhance fraud detection by continuously monitoring, detecting anomalies, creating predictive risk scores, and enabling automated oversight. The literature also indicates that, without robust institutional accountability, governance processes, and internal control structures, analytics alone can't guarantee reliable financial reporting or fraud management.

The results also suggest that the best oversight contexts are those whose analytics and internal controls are seen as a cohesive system, not distinct functions. Although AI, automation, RegTech, and predictive monitoring technologies are transforming financial oversight, their impact is still very much tied to their data quality, explainability, governance maturity, and human oversight. The consistency of analytics-driven oversight remains a challenge due to issues around model reliability, regulatory compliance, cybersecurity, and implementation gaps across institutions.

Overall, the future of fraud detection and financial reporting integrity in U.S. financial systems will depend not only on technological advancement, but also on the ability of institutions to maintain transparent, auditable, and well-governed control environments capable of adapting to increasingly complex financial risks.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

- [1] Abikoye, B. E., Akinwunmi, T., Adelaja, A. O., Umeorah, S. C., & Ogunsuji, Y. M. (2024). Real-time financial monitoring systems: Enhancing risk management through continuous oversight. *GSC Advanced Research and Reviews*, 20(1), 465-476.
- [2] Adeboye, E. O., Ifeanyi, E. V., & Labisi, G. B. E. M. I. S. O. L. A. (2021). Redesigning internal controls for small enterprises: A coso-based framework for fraud prevention and regulatory compliance. *Iconic Research and Engineering Journals (IRE Journals)*, 4(9), 334-344.
- [3] AL-dalmi, A. S. J., & Qader, M. Y. (2021). The Effect COSO Internal Control System in Reducing the Financial Risks related to Financial Statements. *Turkish Online Journal of Qualitative Inquiry*, 12(9).
- [4] Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., ... & Saif, A. (2022). Financial fraud detection based on machine learning: a systematic literature review. *Applied Sciences*, 12(19), 9637.
- [5] Álvarez-Foronda, R., De-Pablos-Heredero, C., & Rodríguez-Sánchez, J. L. (2023). Implementation model of data analytics as a tool for improving internal audit processes. *Frontiers in Psychology*, 14, 1140972.
- [6] Amoako, David & Boboye, Cynthia & Boateng, Victor & Laryea, Jehu. (2025). Artificial Intelligence And Machine Learning For Fraud Detection In The U.S. Banking Industry: Regulatory Frameworks, Implementation, And Challenges. *EPRA International Journal of Economics, Business and Management Studies*. 57-69. 10.36713/epra23647.
- [7] Amoakoh, Christian & Nwinyi, Ifeyinwa & Ampofo, Issabella. (2026). Ai-Enabled Assurance Frameworks: A Review Of Intelligent Systems Enhancing Accuracy And Independence In U.S. Financial Auditing. *Epra International Journal of Economics Business and Management Studies*. 154. 10.36713/epra26251.
- [8] Ampofo, Issabella & Amoakoh, Christian. (2026). Intelligent Risk Monitoring Systems: A Review of Machine-Learning Tools Advancing Early Detection of Financial Irregularities in U.S. Markets. 10.71097/IJAIDR.v17.i1.1729.
- [9] Aobdia, D., Li, E. X., Ramesh, K., & Shen, M. (2025). Deciphering the PCAOB inspection process: Evidence and predictive insights from public data. *Management Science*.
- [10] Bower, M., Godasu, R., Nyakundi, N., & Reynolds, S. (2024, May). Optimizing machine learning data pre-processing for financial fraud detection. In *2024 IEEE International Conference on Electro Information Technology (eIT)* (pp. 028-037). IEEE.
- [11] Celestin, M. (2020). The Role of Data Analytics in Enhancing the Effectiveness of Audit Procedures and Financial Statement Reviews. *Brainae Journal of Business, Sciences and Technology*, 4(8), 835-845.
- [12] Ding, Y. (2023, November). Auditing and assurance: ensuring financial integrity and transparency. In *2023 International Conference on Finance, Trade and Business Management (FTBM 2023)* (pp. 212-218). Atlantis Press.
- [13] Emefa, Jehu & Brakye, Kingsford. (2025). Modernizing General Ledger Reconciliation Standards: Reducing Systemic Risk in Financial Reporting Across Public and Private Sectors. 10.5281/zenodo.17313241.
- [14] Gkegkas, M., Kydros, D., & Pazarskis, M. (2025). Using data analytics in financial statement fraud detection and prevention: A systematic review of methods, challenges, and future directions. *Journal of Risk and Financial Management*, 18(11), 598.
- [15] Gupta, P. P., Sami, H., Zhang, J. H., & Zhou, H. (2025). Does the 2013 COSO internal control framework improve the information environment in the US capital markets?. *Managerial Auditing Journal*, 40(4), 357-383.
- [16] Homer, E. M. (2020). Testing the fraud triangle: a systematic review. *Journal of financial crime*, 27(1), 172-187.
- [17] Kaawaase, T. K., Nairuba, C., Akankunda, B., & Bananuka, J. (2021). Corporate governance, internal audit quality and financial reporting quality of financial institutions. *Asian Journal of Accounting Research*, 6(3), 348-366.

- [18] Krishnan, J., Krishnan, J., & Liang, S. (2020). Internal control and financial reporting quality of small firms: A comparative analysis of regulatory regimes. *Review of Accounting and Finance*, 19(2), 221-246.
- [19] Liu, W. P., & Huang, H. W. (2020). Auditor realignment, voluntary SOX 404 adoption, and internal control material weakness remediation: Further evidence from US-listed foreign firms. *International Business Review*, 29(5), 101712.
- [20] Malysheva, O. A. (2020). Fraud Detection and AML Analytics in Real-Time Payment Systems.
- [21] Minkkinen, M., Laine, J., & Mäntymäki, M. (2022). Continuous auditing of artificial intelligence: a conceptualization and assessment of tools and frameworks. *Digital Society*, 1(3), 21.
- [22] Mohammed, M. A., Al-Abedi, T. K., Flayyih, H. H., & Mohaisen, H. A. (2021). Internal control frameworks and its relation with governance and risk management: An analytical study. *Studies of Applied Economics*, 39(11).
- [23] Mudawanah, S., Fatimah, I., Nalsal, P., & Purnomo, A. D. (2024). The Role of Continuous Auditing in Enhancing Corporate Governance. *Islamic Studies in the World*, 1(3), 121-130.
- [24] Oguntibeju, O., Adonis, M., & Alade, J. (2024). Systematic review of real-time analytics and artificial intelligence frameworks for financial fraud detection. *International Journal of Advanced Research in Computer and Communication Engineering*, 13(9).
- [25] Owolabi, O. S., Uche, P. C., Adeniken, N. T., Ihejirika, C., Islam, R. B., Chhetri, B. J. T., & Jung, B. (2024). Ethical implication of artificial intelligence (AI) adoption in financial decision making. *Computer and Information Science*, 17(1), 1-49.
- [26] Pallapati, Joshua & Oman-Amoako, Matthew. (2026). Artificial Intelligence And Ethical Risk Governance In Financial Decision-Making: Examining Fairness, Accountability, And Policy Alignment. *Epra International Journal of Economics Business and Management Studies*. 77. 10.36713/epra26817.
- [27] Rashid, C. A. (2022). The role of internal control in fraud prevention and detection. *Journal of Global Economics and Business*, 3(8), 43-55.
- [28] Sánchez-Aguayo, M., Urquiza-Aguilar, L., & Estrada-Jiménez, J. (2021). Fraud detection using the fraud triangle theory and data mining techniques: A literature review. *Computers*, 10(10), 121.
- [29] Sodnomdavaa, T., & Lkhagvadorj, G. (2025). Financial statement fraud detection through an integrated machine learning and explainable AI framework. *Journal of Risk and Financial Management*, 19(1), 13.
- [30] Svetlova, E. (2022). AI ethics and systemic risks in finance. *AI and Ethics*, 2(4), 713-725.
- [31] Tiwari, R. (2023). The application of AI and machine learning in the financial industry and its effects on risk management and fraud detection. *International Journal of Scientific Research In Engineering And Management*, 7(1), 1-12.
- [32] 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.
- [33] Weickgenannt, A. B., Hermanson, D. R., & Sharma, V. D. (2021). How US audit committees oversee internal control over financial reporting. *International Journal of Auditing*, 25(1), 233-248.
- [34] Westland, J. C. (2020). *Audit Analytics* (Vol. 84). Springer, ctp.
- [35] Yeboah, Mary & Agyei, Evelyn & Anim, Barnabas & Nartey, Olivia & Nwinyi, Ifeyinwa. (2026). AI in Financial Auditing: Addressing U.S. Audit Failures and Strengthening PCAOB/SEC Compliance. 05. 23-32. 10.5281/zenodo.18188728.
- [36] Zhou, J. (2020). Continuous audit data analytics and internal control intelligence (Doctoral dissertation, Rutgers University-Graduate School-Newark).