The role of artificial intelligence in auditing: enhancing accuracy and reducing fraud in the post-pandemic era

Dr. Mohit Bhardwaj[1*] and Dr. Pankaj Yadav[2]

[1] Assistant Professor, Department of Commerce, Ganna Utpadak Degree College, Baheri, Bareilly, Uttar Pradesh, India

[2] Associate Professor, Department of Commerce, Bareilly College, Bareilly, Uttar Pradesh, India

Correspondence Author: Dr. Mohit Bhardwaj

Received 18 Sep 2024; Accepted 31 Oct 2024; Published 5 Nov 2024

DOI: https://doi.org/10.64171/JAES.4.4.33-38

Abstract

The COVID-19 pandemic accelerated digital transformation throughout business and financial ecosystems; auditing was no exception. With remote working, distributed data sources, and rapidly changing risk landscapes, auditors confronted both logistical constraints and novel fraud risks. Artificial intelligence (AI) — including machine learning (ML), natural language processing (NLP), anomaly detection, and robotic process automation (RPA) — has emerged as a pivotal technology to help auditors enhance evidence-gathering, automate routine procedures, and detect sophisticated fraud patterns that are difficult to find with traditional sampling techniques. This paper analyses how AI has changed audit methodologies in the post-pandemic era, assesses its capacity to improve accuracy and fraud detection, identifies practical and ethical challenges (such as model bias, explainability, and governance), and proposes a framework for safe, effective, and regulated AI adoption in audit practice. The study uses a mixed-methods approach: a systematic review of literature up to 2024; policy and standards analysis (including pandemic audit-guidance); and case-based illustrations from Big Four and large-firm implementations. Key findings indicate that AI tools can increase anomaly detection rates, expand population testing beyond statistical samples, and shorten time to detection for unusual transactions — but these gains depend on data quality, model selection, interpretability, and robust governance. Independent reviews and regulatory bodies have observed that firms often lack metrics to evaluate AI's impact on audit quality and rarely maintain formal monitoring of algorithmic performance and risk. Ethical concerns—algorithmic bias, over-reliance on automation, model drift, and opaque decision-making—are material and require both technical and procedural safeguards. Effective adoption requires harmonizing technology with auditing standards, enhancing auditor capabilities (data science literacy), instituting continuous model validation and performance metrics, and creating a layered governance model that ties AI outputs to professional skepticism and human oversight. Policy recommendations include: (1) standardized AI-audit performance metrics and reporting; (2) mandatory documentation and explainability requirements for AI tools used in substantive procedures; (3) third-party or regulator-led audits of AI systems (AI-audit of audit tools); (4) auditor upskilling programs and interdisciplinary teams; and (5) alignment between professional standards and technology risk frameworks. The paper concludes that while AI has strong potential to both enhance audit accuracy and reduce fraud in the post-pandemic environment, the benefits will materialize sustainably only if auditing firms, standard setters, and regulators collaborate to ensure transparent, accountable and validated use of AI.

Keywords: artificial intelligence, auditing, fraud detection, machine learning, anomaly detection, post-pandemic auditing, audit quality, explainability, governance

Introduction

1. Background: pandemic shocks and auditing transformation

The COVID-19 pandemic (beginning early 2020) brought unprecedented disruption to business operations, supply chains, and financial reporting environments. For auditors, the pandemic produced two overlapping effects: first, traditional audit procedures that depended on physical inspection, face-to-face confirmations, and in-person sampling became impractical; second, economic stress and rapid operational changes increased the risk of misstatement and fraud. Standard setters and professional bodies thus issued guidance to help auditors adapt their procedures to the remote environment, highlighting the need for alternative evidence and enhanced professional judgment. The International Auditing and Assurance Standards Board (IAASB) and global professional organizations published specific guidance focused on maintaining audit quality during the pandemic, recommending alternative procedures and emphasizing the importance of sufficient, appropriate evidence despite changed circumstances [1].

In parallel, firms accelerated their adoption of digital tools — cloud platforms, data lakes, analytics, and AI-enabled systems — to permit remote working and automated handling of massive, heterogenous datasets. This shift created an opportunity for AI technologies to address both logistical constraints and heightened fraud risk by enabling continuous monitoring, improved pattern recognition, and automated extraction of evidence from unstructured documents (e.g., contracts, emails, invoices). Yet, this rapid adoption also raised concerns: how would AI-driven outputs align with auditing standards that assume professional skepticism and human judgment? What would auditors do to confirm AI models and are they not going to create a bias and make the audit trail less transparent? These questions came to focus on the post-pandemic changes in audits [2].

2. Defining AI in the audit context

Within an auditing context, the term AI can be used to refer to a collection of algorithms that are used to derive information about data and automate decision-support processes. Such area as supervised and unsupervised machine learning algorithms (e.g. random forests, gradient boosting, neural networks), anomaly detection algorithms, natural language processing (NLP) to review documents, invoice/receipt imaging using computer vision, and repetitive process robotics and automation are also key techniques. Each technique has a different affordance: NLP helps process unstructured text (contracts, minutes), ML models find anomalous transaction patterns, and RPA automates data retrieval and routine reconciliations. Combined, these capabilities not only allow the auditor to have a wider scope of testing beyond samples to population-level analytics and close to real-time monitoring [3].

3. Why AI matters for accuracy and fraud detection

The traditional auditing is often based on the statistical sampling and the examination of exceptions by regulations. Although these techniques have worked well in the past, they may fail to detect non-obvious, adaptive fraud patterns that are few when compared to big data volumes or when other systems are exploiting non-obvious correlations. AI improves the process of detection in several aspects:

a) **Population-level analysis:** ML algorithms can process large-scale populations of transactions, identifying outliers and clusters of suspicious transactions, which sampling can overlook.

b) **Pattern recognition:** Advanced models detect the non-linear, complex relationships (e.g., vendor networks, time series patterns of transactions) that are signals of collusion or synthetic fraud.

c) **Unstructured data parsing:** NLP identifies the important clauses, anomalous words or moods in the contracts and correspondences that can be indicative of aggressive accounting or hiding.

d) **Ongoing auditing:** Automated practices will allow recognizing anomalies and act on it faster, allowing it to be investigated earlier.

e) **Efficiency gains:** Automation reduces time spent on repetitive tasks and allows auditors to allocate judgmental work to higher-risk areas.

Empirical and practitioner reports indicate substantial improvements in detection and efficiency when AI is correctly implemented. For example, leading professional services firms report AI-based tools that scan general ledger data and other source systems to produce anomaly visualizations and candidate flags for auditor follow-up — shortening time to detection and expanding audit coverage. Nonetheless, the assertions of the definite percentage improvements should be considered very carefully and within context: improvements are strongly tied to data availability, preprocessing, feature engineering, and the governance of the use of the models [4].

4. The post-pandemic landscape: opportunities and new risks

The recent period after the pandemic is being defined by long-term hybrid work patterns, the growing use of the cloud, and ongoing supply-chain and economic instability. The following conditions motivate and make AI implementation in audit more complicated:

- **Opportunity:** The availability of richer datasets to AI algorithms is possible due to distributed data sources and digital trail of transactions. The centralization of data lakes helps the firms to scale analytics and make cross-entity analysis and transaction linkage possible.
- **Risk:** Remote operations and API-based integrations create new loopholes to commit fraud (compromised credentials, synthetic vendors). The opponents also may use AI to generate more believable forgeries or spam-assisted social engineering. Further, model drift (the variations in the data distributions with time) may deteriorate the detection performance unless it is observed [4].

5. Governance, ethics, and professional standards alignment

The governance gap is another theme that has been present in both literature and regulatory commentary: companies tend to implement AI tools without carefully quantifying their impact on the quality of audits. Independent reviews have observed that the vast majority of large companies do not have any official measures that would determine the quality impact of AI, and the monitoring is frequently restricted to usage rates instead of performance indicators or error monitoring. This implies that an AI model could be used in a large scale with no obvious facts that it enhances the audit results or controls against systematic bias. To enhance the accountability and professional scepticism standards bodies and regulators have demanded increased transparency, model documentation, and human control [5].

Key governance elements include:

- **Model validation and continuous monitoring:** formal mechanisms to test accuracy, false positive/ negative rates and time stability.
- **Explainability:** the capacity to give explainable rationales to flagged transactions so that the auditors can exercise judgment.
- **Data governance:** access controls, quality checks, and lineage.
- **Audit trail and reproducibility:** records that connect AI results with uncooked evidence and audit findings.
- **Human-in-the-loop:** making decisions and embedding professional judgment instead of just being strictly automated.

6. Research objectives

This paper aims to:

a) Synthesize the state of art in AI-enabled auditing up to 2024, emphasizing fraud detection capabilities and documented outcomes.

b) Evaluate practical impediments to reliable AI adoption (data quality, model interpretability, governance, regulatory compliance).

c) Analyse post-pandemic shifts that alter both the demand for AI and the threat landscape.

d) Propose a governance and measurement framework to help firms realize AI's potential while safeguarding audit quality and ethics.

The analysis is based on the review of scholarly articles, industry whitepapers, standards-board directions, and practitioner reports to 2024. Empirical research on AI in auditing, IAASB and IFAC policy references on the question of pandemic and technology (as well as technology, in general), practitioner-focused case studies (e.g., Big Four AI projects), and recent references on the topic of algorithmic bias and ethics are all considered core references [6].

Literature review

This is a literature review that identifies exemplary scholarly and practitioner work. Each of the entries provides a short overview of the main argument and applicability to AI in auditing and fraud detection.

a) **Kokina & Davenport (2017)** —Kokina and Davenport discussed the first uses of data analytics and machine learning in audit practice, where the authors suggest that analytics can transform how auditors sample in an audit into full-population testing and enable continuous auditing. Their piece of work established a background to the later studies by outlining the possible efficiency enhancement and auditor skills development requirements. *(Kokina & Davenport, 2017)* [7].

b) **Alles (2015 & subsequent reviews)** — Miklos Alles and others gave a detailed examination of ongoing use of auditing and analytics, including the necessity of infrastructure and the contribution of the information systems in support of AI-based methodologies. Their study highlights the long-standing demands to adopt integrated data structures to aid AI. *(Alles, 2015; subsequent updates)* [8].

c) **PwC (2022–2023 whitepapers)** — PwC reported on their forensic and AI speeches on actual use of AI in fraud detection and reported enormous improvements in detection speed and coverage and noted that AI could be used by bad actors. The GL.ai and other tools provided by PwC is a demonstration of how commercial audit tools use ML to general ledger analytics. *(PwC, 2022–2023)* [9].

d) **IFAC / IAASB guidance (2020)** — IAASB and IFAC provided guidance on the pandemic in regards to alternative audit procedures and remote gathering of evidence. Although these documents are not AI-specific, they hastened the use of digital tools and helped to understand that standards must have enough adequate evidence no matter the approach. *(IAASB/IFAC, 2020)* [10].

e) **Murikah et al. (2024) — bias and ethics** — Recent scholarly research has concentrated on AI-applied auditing as relates to the concept of bias and explainability in algorithms, as well as the risks associated with ethical concerns. Murikah (2024) plots sources of bias, opaqueness of complex models, and down stream impact on audit judgments, calling on high quality governance and equity. *(Murikah, 2024)* [11].

f) **Emerald/International Journal of Accounting articles (2023–2024)** — The articles present case studies of the AI application in risk assessment and transaction testing, which report enhanced anomaly detection, though there is no clear evidence of a strong audit quality validation. Such examples confirm the need of performance indicators and human control. *(Various, 2023–2024)* [12].

g) **Regulatory reviews (FRC / public watchdogs) (2024)** — The reviews by regulators found a weakness in governance: as firms are using AI tools, they fail to gauge the effect of the tools on audit quality. The UK Financial Reporting Council (FRC) discovered that there was a lack of formal monitoring and suggested more explicit mechanisms of overseeing. *(FRC, 2024)* [13].

h) **Systematic reviews and meta-analyses (2021–2024)** — Some of the systematic literature reviews were able to synthesize research on AI methods (ML, NLP, anomaly detection), and its application in auditing, finding common themes: models performance is good; current obstacles are data imbalance, no labelled fraud data, model interpretability and integration with existing audit processes. *(Systematic reviews, 2021–2024)* [14].

Methodology

Research design and approach

This paper adopts a mixed-methods research design combining:

a) **Systematic literature synthesis:** A structured review of peer-reviewed articles, working papers, industry whitepapers, and regulator reports up to 2024. Keywords used included "AI in auditing," "machine learning fraud detection auditing," "NLP contract analysis audit," and "audit analytics." Sources were selected for relevance, recency (≤2024), and influence (citations, regulator adoption, or industry uptake). Such major databases and sources as Scopus, ScienceDirect, SSRN, whitepapers of professional firms (PwC, Deloitte), and professional bodies (IAASB, IFAC) were utilized.

b) **Policy and standards analysis:** An overview of and comparative analysis of pandemic-era audit guidance (IAASB/IFAC), standard-setting commentary and regulator reviews (e.g., FRC) to learn what is expected of other processes and tool governance in crisis situations.

c) **Practitioner cases examples:** Case descriptions of AI-tools (e.g., GL.ai by PwC), which are publicly available, and reports of firms were reviewed to demonstrate live examples, their alleged benefits, and governance. These were practical illustrations as opposed to controlled empirical case studies.

d) **Thematic synthesis and structure development:** The results of the literature and the cases were synthesized to identify common themes (accuracy, fraud detection, governance, ethics) and suggest a governance and measurement framework of AI in audit practice.

Data selection and inclusion criteria

- **Temporal scope:** Documents and literature published until 2024.
- **Types of sources include:** Peer-reviewed research paper, preprints containing substantive methods, professional firm whitepapers, reports of a regulatory agency, and standards guidance. Non-public proprietary datasets or internal firm audits were excluded unless summarized in public documents.

Limitations of the methodology

- **Absence of primary empirical data:** The study does not include new experimental tests or proprietary firm performance datasets; conclusions rely on published results and practitioner reports.
- **Publication bias:** The vendors or consulting firms might selectively publish only reports of positive implementation; to counteract this view, regulator reviews and academic critiques were incorporated.
- **The field is changing fast:** AI-based tools and regulatory provisions change rapidly; the deadline set to 2024 implies that there is a significant risk of missing very recent changes after 2024.

Ethical considerations

All sources used are publicly available. No human subjects or confidential client information were used. The methodology focuses on triangulation, or the comparison of academic evidence, reviews by regulators, and reports by practitioners to minimize single-source prejudice.

Description

1. **Practical ways AI enhances audit accuracy and fraud detection**

1.1 **Population-level anomaly detection:** AI allows auditors to use full populations of transactions, as opposed to just sampling. Trained models trained on labeled exceptions (where possible) and unsupervised anomaly detection (e.g., isolation forests, clustering) may indicate unusual features in a transaction: unusual vendor sequence, round-number invoice amounts, price variances, or unusual timing in relation to business cycles. Population testing reduces sampling risk and increases the chance of detecting rare but material fraudulent activities. Practitioner tools (e.g., GL.ai) illustrate the translation of these capabilities into audit workflows by scanning ledgers and highlighting candidate anomalies for auditor review.

1.2 **NLP for contracts, minutes and email evidence:** A large portion of audit evidence is unstructured text. NLP techniques (named entity recognition, clause extraction, semantic similarity) accelerate review of contracts, board minutes, and communications. An example is that AI is able to spot abnormal clauses that give one-time approvals, or find related-party names, or even sentiment change in management conversation that could be associated with risk. This reduces manual review time and enables auditors to focus on high-risk textual evidence.

1.3 **Network analysis and link detection:** ML based on graphs can identify missing networks or transaction sequence similar to collusion by vendors. Graphs of entities (vendors, approvers, accounts) can be formed and with algorithms, closely knit clusters can be identified or bridge nodes that could have been overlooked by traditional processes can be identified. This type of network analytics can be especially valuable in a scheme related to fraudulent shell companies or difficult relationships with vendors.

1.4 **Continuous monitoring and near-real-time alerts:** Continuous controls monitoring (CCM): AI systems can be incorporated into continuous controls and used to issue near real time exceptions to allow quicker investigation and mitigation. With more real-time finance operations in the organizations after the pandemic, the auditors acquired the chance to switch to continuous assurance models instead of periodic testing.

Table 1: Representative AI techniques and audit applications

AI technique	Typical audit application	Benefit
Supervised ML (RF, XGBoost)	Fraud classification on labeled historic fraud instances	High predictive power where labeled data exists
Unsupervised anomaly detection	Outlier transactions, rogue vendor activity	Detects novel or rare anomalies without labels
NLP (NER, clause detection)	Contract review, minutes analysis	Automates unstructured evidence parsing
Graph/network analysis	Detect collusion / vendor rings	Reveals relational fraud patterns
RPA (with ML)	Data extraction and reconciliation	Automates repetitive tasks; frees judgmental time

(***Sources:*** practitioner whitepapers and systematic reviews) [15].

2. **Empirical evidence and limits: what the literature shows**

Empirical literature and systematic reviews until 2024 point to some observable improvements in detection rates and efficiency but focus on caveats:

- **Performance dependence on data quality:** The absence of fields, ambiguous naming of vendors and the absence of labeled cases of fraud undermine model reliability. (Systematic reviews).
- **Imbalanced datasets:** Fraud is a rare event; class imbalance biases traditional supervised models. Oversampling, synthetic minority oversampling (SMOTE) or anomaly detection techniques are used but are limited in one way or another. (Academic reviews).
- **Tradeoffs in interpretability:** Simple models (deep learning) may be worse than complex models, but they are more explainable. Explainability is important with regards to audit evidence since auditors should be able to explain

why they investigated a transaction. (Ethics & bias literature).

Practitioner reports (e.g., PwC, Deloitte) indicate that anomaly discovery and efficiency have been fundamentally improved, although reviews by independent regulators note that companies seldom measure the effect of AI on audit quality using formal measures. The observation implies that any positive practitioner narratives can surpass serious internal review.

3. Risk picture: bias, model drift, adversarial threats

3.1 Algorithmic bias and fairness: The systems that are trained based on the past data might acquire systemic biases (ex: some business units wrongly labeled as low-risk in the past). Distorted false-positive figures may cause unreasonable suspicion of particular agents and unnecessary investigation work. Research suggests fairness testing and counterfactual to determine disparate impacts.

3.2 Model drift and retraining needs: Due to the changing business processes, models may drift out of initial distributions to lower the accuracy.Continuous monitoring and periodic retraining on fresh labeled data are required. Without processes for monitoring, firms risk blind faith in stale models.

3.3 Adversarial manipulation and AI-enabled fraud: AI can help fraudsters too: synthetic data generation, deepfakes, and automated phishing make detection harder. Firms must anticipate adversarial tactics and include robustness testing and multi-modal corroboration (cross-system signals) to limit false negatives.

4. Governance and assurance of AI tools

Such a strong governance structure is necessary because of the stakes and risks involved. The suggested layered model of governance is the combination of technical validation, operational controls, and regulatory reporting:

Layer 1: Data Governance: to provide consistent inputs, lineage, quality rules, access controls, and master data management.

Layer 2: Model Governance: version control, validation data, performance KPIs (precision, recall, AUC), bias/fairness tests, and change management.

Layer 3 — Operational Controls: AI denies access based on role-based, human-in-the-loop validation, escalation policies to reported high-risk items.

Layer 4 — External Assurance and Reporting: third-party audit of AI systems periodically, regulatory disclosures with respect to AI use and metrics reported to audit committees/regulators.

This framework concurs with regulator review calls to quantify the effects of AI on the quality of audits and to record the oversight procedures.

5. Auditor competences & organizational implications

The application of AI requires the change within an organization:

- **Upskilling auditors:** Data literacy and basic ML knowledge and understanding the AI output should be taught to auditors so that they can exercise professional skepticism on AI flags.
- **Interdisciplinary teams:** One should combine audit specialists, data scientists, and IT controls to achieve technical validity and audit relevance.
- **Process redesign:** The working processes should be modified with model output, follow-up procedures, and decision documentation to maintain the integrity of audit trails.

6. Proposed measurement and reporting metrics (practical KPIs)

To measure the contribution of AI tools to the quality of audits, firms are to monitor the following KPIs:

- **Detection precision at top N flagged items:** Detection precision at top N flagged items.
- **Recall (coverage) on historical known fraud cases:** how many historical frauds would have been flagged.
- **Time to detection:** median time from occurrence to flag.
- **False positive workload:** average number of false positives per audit hour.
- **Model stability:** retraining cycle AUC/precision changes.

Frequent reporting of these KPIs to audit committees and regulators will show responsibility and would give evidence of quality improvement.

7. Regulatory & standard-setter implications

Regulators and standards boards (IAASB, IFAC) can take a number of measures:

- **Documentation guidance:** what model auditors need to keep (training data description, validation results, feature importance).
- **Performance reporting:** make AI performance KPIs periodic reporting to supervisory authorities mandatory.
- **Third-party assurance of AI tools:** an independent assurance framework on AI tools may be created just like the SOC reports of cloud providers.

9. Concluding synthesis

AI holds powerful capabilities to enhance audit accuracy and detect fraud more effectively than many traditional methods — particularly in an era where remote operations and digital transaction volumes have grown post-pandemic. However, realizing these benefits sustainably requires disciplined data governance, continuous model validation, transparent documentation, human oversight, and clear regulatory expectations. Firms must shift from tool adoption to accountable AI integration with measurable outcomes tied to audit quality.

Regulator reviews up to 2024 indicate the profession is at an inflection point: widespread experimentation and adoption are underway, but formal evaluation and governance lag. If the profession, standards setters, and regulators coordinate to create interoperable governance and reporting standards, AI can be an enduring force for better audits and stronger fraud deterrence.

References

1. Alles M. Continuous auditing: theory and application, 2015.
2. Deloitte. How artificial intelligence is transforming the financial services industry. Deloitte Insights [Internet]. [cited 2026 Feb 26]. Available from: https://www.deloitte.com/ng/en/services/consulting-risk/services/how-artificial-intelligence-is-transforming-the-financial-services-industry.html
3. Emerj. Artificial intelligence at PwC—two use cases. Emerj [Internet], 2023 [cited 2026 Feb 26]. Available from: https://emerj.com/ai-at-pwc-two-use-cases/
4. Financial Reporting Council (FRC). Review: AI usage and impact on audit quality. London: FRC, 2024.
5. International Auditing and Assurance Standards Board (IAASB). Guidance for auditors during the COVID-19 pandemic [Internet], 2020 [cited 2026 Feb 26]. Available from: https://www.iaasb.org/focus-areas/guidance-auditors-during-covid-pandemic
6. International Federation of Accountants (IFAC). Summary of COVID-19 audit considerations [Internet], 2020 [cited 2026 Feb 26]. Available from: https://www.ifac.org/knowledge-gateway/discussion/summary-covid-19-audit-considerations
7. Kokina J, Davenport T. The emergence of artificial intelligence and analytics in accounting and auditing, 2017.
8. Murikah W. Bias and ethics of AI systems applied in auditing, 2024. Available from: https://www.sciencedirect.com/science/article/pii/S2468227624002266
9. PwC. Impact of artificial intelligence on fraud and scams. London: PwC, 2022/2023. Available from: https://www.pwc.co.uk/forensic-services/assets/impact-of-ai-on-fraud-and-scams.pdf
10. Artificial intelligence in auditing: systematic reviews and meta-analyses, 2023-2024.
11. Scholarly and practitioner articles on AI and auditing practices. Emerald; International Journal of Accounting, 2023-2024.
12. Guidance for Auditors During the COVID Pandemic | IAASB.
13. How Artificial Intelligence is Transforming the Financial Services Industry.
14. (PDF) Artificial Intelligence in Auditing: A Systematic Review of Tools, Applications, and Challenges.
15. Artificial Intelligence at PwC - Emerj Artificial Intelligence Research.
16. How Artificial Intelligence is Transforming the Financial Services Industry.
17. (PDF) Artificial Intelligence in Auditing: A Systematic Review of Tools, Applications, and Challenges.
18. Challenges and opportunities for artificial intelligence in auditing: Evidence from the field – ScienceDirect.
19. Auditors in the digital age: a systematic literature review | Digital Transformation and Society | Emerald Publishing.
20. Impact of Artificial Intelligence on Fraud and Scams.
21. Guidance for Auditors During the COVID Pandemic | IAASB.
22. Bias and ethics of AI systems applied in auditing - A systematic review – ScienceDirect.
23. The role of artificial intelligence in auditing and fraud detection in accounting information systems: moderating role of natural language processing | International Journal of Organizational Analysis | Emerald Publishing.
24. (PDF) Artificial Intelligence in Auditing: A Systematic Review of Tools, Applications, and Challenges.
25. Impact of Artificial Intelligence on Fraud and Scams.