IJAAR PUBLISHING®

West African Journal of Interdisciplinary Research | ISSN: 3027-1878
Volume 4, Issue 1 (2026) | www.ijaar.org

METHODOLOGIES FOR IMPLEMENTING AI-POWERED AUDITING

Famous E. Akpore
Department of Computer Science,
School of Science and Technology
Delta State Maritime Polytechnic, Burutu Nigeria.
Email: akporefamous@gmail.com

Abstract

Artificial intelligence (AI) is redefining assurance by automating evidence collection, anomaly detection, and continuous risk monitoring. Yet most organizations struggle to move from pilots to repeatable, controlled AI-enabled audit programs. This paper synthesizes leading standards (NIST AI RMF, ISO/IEC 23894) and emerging regulatory expectations (EU AI Act) to propose a practical, end-to-end methodology for AI-powered auditing. We present a lifecycle covering audit opportunity discovery, data readiness, model governance, control design, assurance procedures, and performance evaluation. We also provide implementation patterns, control checklists, and KPIs that enable internal and external auditors to operationalize trustworthy AI in financial, operational, and compliance audits. Case vignettes illustrate how to deploy model cards, risk registers, and continuous controls monitoring in enterprise settings.

KEYWORDS: Artificial Intelligence, Auditing, Assurance, Risk Management, Governance

https://doi.org/10.46654/zd4j8365

Introduction

Audit functions increasingly apply machine learning (ML) and large language models (LLMs) to journal-entry testing, segregation-of-duties analysis, vendor screening, and policy compliance. Benefits include increased coverage, near real-time monitoring, and the ability to surface complex, non-linear risk signals from high-volume data. However, these gains must be balanced against new risks such as model bias, concept drift, hallucination, privacy breaches, and control circumvention. Auditors need a disciplined implementation methodology that aligns with established risk and control frameworks while remaining technology-agnostic.

Statement of the problem

Although AI has demonstrated potential in revolutionizing audit practice, most organizations struggle with implementation due to, lack of structured methodologies, concerns over model transparency, explainability and bias, inconsistent data quality and governance, and uncertainty about compliance with evolving regulatory standards. These gaps create barriers to achieving trust, reliability, and scalability in AI-enabled audit systems.

Objectives

The main objective of this study is to explore methodologies suitable for implementing AI-powered auditing. Specifically, this paper seeks to:

i. Propose a structured methodology for implementing AI in auditing.
ii. Identify challenges and risks associated with AI-powered auditing.
iii. Highlight relevant standards and frameworks for trustworthy AI.
iv. Provide recommendations for auditors, regulators, and organizations adopting AI.

4. Methodology for Implementing AI-Powered Auditing

4.1. Governance and Program Setup

i. Establish an AI Audit Charter aligned to enterprise risk appetite and the Three Lines Model.
ii. Define roles: model owner, product owner, data steward, MLOps engineer, AI control tester, and audit sponsor.
iii. Approve an AI risk taxonomy (safety, bias/fairness, privacy, robustness, resilience, cybersecurity, explainability, legal/regulatory).
iv. Adopt or profile a reference framework (NIST AI RMF functions: Map–Measure–Manage–Govern) and ISO/IEC 23894 processes.
v. Maintain an AI system inventory, risk register, and a policy for general-purpose and third-party models.

4.2. Audit Use-Case Discovery and Prioritization

i. Build a use-case backlog; score items on materiality, control objectives, data availability, and model feasibility.
ii. Select quick wins (e.g., duplicate payments, vendor sanctions screening) and strategic bets (e.g., narrative analytics of contracts).

4.3. Data Readiness and Controls

i. Data mapping and lineage across ERP, G/L, AP, HR, and procurement systems.

ii. Data quality controls: completeness, accuracy, timeliness, validity, uniqueness. Privacy and confidentiality: data minimization, masking, purpose limitation, retention, and lawful basis.
iii. Establish reference datasets and drift monitors for streaming sources.

4.4. Model Development and Documentation

i. Select algorithms consistent with audit objectives and explainability needs (e.g., tree-based models for interpretable anomaly scores).
ii. Establish model documentation (Model Cards): intended use, training data, limitations, performance across sub-populations, monitoring plan.
iii. Partition datasets with strong segregation of test/validation; adopt cross-validation; log feature importance and counterfactual explanations.
iv. Stress-test for bias, robustness to adversarial inputs, and sensitivity to concept/seasonality drift.

4.5 Control Design for AI Systems

1. Preventive: access management to models and features; CI/CD gates for model deployment; data protection by design.
2. Detective: model performance and drift thresholds; human-in-the-loop review; logging and immutable audit trails; provenance/watermark checks.
3. Corrective: rollback procedures, kill-switches, and documented remediation workflows.
4. Governance: periodic model risk assessments; independence of validation; third-party risk management; regulatory alignment (e.g., EU AI Act).

4.6. Assurance Procedures and Evidence

1. Plan: define assertions (existence, completeness, accuracy), materiality, tolerable deviation, and sampling strategy augmented with ML-based stratification.
2. Perform: run analytics (e.g., isolation forests) to score transactions; test exceptions with dual-control review; confirm external evidence where applicable.
3. Evidence: retain datasets, code snapshots, model artifacts, and decision logs as audit evidence; maintain traceability from finding to data and model version.

4.7 Deployment, Monitoring, and Continuous Assurance

1. Integrate with ticketing/issue management; automate alert routing; define SLOs for investigation and closure.
2. Monitor fairness, drift, and false-positive rates; recalibrate thresholds by seasonality; conduct post-implementation reviews.

4.8. Metrics and KPIs

Coverage (population vs. sample), precision/recall of exception flags, mean time-to-detect and remediate, control effectiveness uplift, cost-per-exception investigated, and user adoption.
Include balanced scorecards that reflect both risk reduction and operational efficiency.

5. Justification

The methodology provides auditors with a disciplined framework to adopt AI responsibly. By aligning with international standards and emerging regulations (European Union, 2024), organizations can balance efficiency gains with trustworthiness, mitigating risks of bias, non-compliance, and audit failure.

6. Literature

The application of AI in auditing has been widely discussed across academic, professional, and regulatory domains. Researchers argue that AI fundamentally transforms the assurance process by shifting from retrospective sampling methods to predictive and continuous auditing approaches. According to NIST (2023), the AI Risk Management Framework emphasizes that risk management is central to AI deployment in sensitive fields such as auditing, highlighting mapping, measuring, and managing risks as core principles. ISO (2023) provides detailed guidelines through ISO/IEC 23894, stressing the need for governance structures, bias detection, and lifecycle monitoring to ensure trustworthy AI. The European Union (2024) established the AI Act, which categorizes certain audit applications of AI as high-risk, thereby mandating strict compliance, transparency, and human oversight measures.

Professional bodies have also contributed to the literature. The Institute of Internal Auditors (2024) developed an AI auditing framework that integrates AI into risk-based audit planning and emphasizes the auditor's role in overseeing machine learning systems. Similarly, ISACA (2024) published toolkits for AI governance, recommending that auditors evaluate not just financial data but also algorithmic decision-making processes, data pipelines, and cybersecurity considerations. Academic research complements these standards. Vasarhelyi et al. (2022) discussed the concept of continuous auditing supported by AI, which allows auditors to perform real-time risk assessments. Mitchell et al. (2019) introduced Model Cards as a transparency mechanism to disclose model performance, intended use cases, and limitations—critical for audit accountability. Furthermore, research by Kokina and Davenport (2017) explored how AI augments professional judgment, cautioning that while automation improves efficiency, ethical concerns and auditor expertise remain indispensable.

Overall, the literature suggests that AI in auditing is not merely a technological shift but also a transformation in governance, ethics, and professional accountability. It highlights the convergence of international standards, professional guidance, and academic research as essential for building robust methodologies for AI-powered auditing.

6. Data preparation and analysis

AI auditing relies on structured and unstructured data from ERP systems, financial statements, procurement records, and HR databases. Data preparation involves cleaning, normalizing, and ensuring data integrity. Analysis leverages supervised and unsupervised machine learning, anomaly detection, and natural language processing for compliance checks. Proper validation ensures that audit findings are accurate, explainable, and reproducible.

7. Findings

i. AI enhances audit efficiency by enabling continuous monitoring and real-time detection of anomalies.
ii. Strong governance frameworks mitigate risks related to transparency and accountability.
iii. Data readiness and quality remain critical determinants of success.
iv. Adoption is limited by organizational readiness, auditor expertise, and regulatory uncertainty.

8. Conclusion

An AI-powered auditing can materially improve assurance coverage and timeliness, but only with robust governance, documented controls, and continuous monitoring. By adopting a lifecycle that integrates NIST AI RMF and ISO/IEC 23894 processes—and by anticipating EU AI Act obligations—audit leaders can scale AI responsibly while preserving independence, evidence integrity, and stakeholder trust.

9. Recommendations

i. Organizations should establish governance structures for AI adoption in auditing.
ii. Auditors must be trained in AI systems and ethical considerations.
iii. Regulators should update audit standards to integrate AI-specific guidelines.
iv. Continuous monitoring mechanisms should be deployed to detect model drift and bias.
v. Collaboration between professional bodies and academia should be strengthened to evolve methodologies.

References

European Union, 'EU Artificial Intelligence Act,' Official Journal of the European Union, July 12, 2024. Available: https://artificialintelligenceact.eu/the-act/

ISACA. (2024). Artificial intelligence audit toolkit and governance resources. ISACA. https://www.isaca.org

ISO/IEC 23894:2023, 'Information technology—Artificial intelligence—Guidance on risk management,' 2023.

Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., Spitzer, E., Raji, I. D., & Gebru, T. (2019). Model cards for model reporting. Proceedings of the Conference on Fairness, Accountability, and Transparency (FAT*19), 220–229. Association for Computing Machinery. https://doi.org/10.1145/3287560.3287596

National Institute of Standards and Technology (NIST), 'Artificial Intelligence Risk Management Framework (AI RMF 1.0),' 2023. Available: https://doi.org/10.6028/NIST.AI.100-1

International Organization for Standardization. (2023). ISO/IEC 23894:2023 Information technology—Artificial intelligence—Guidance on risk management. ISO.

The Institute of Internal Auditors (IIA), 'Artificial Intelligence Auditing Framework,' Sept. 2024 update.