Volume 4 Number 1 (2026)
January – June 2026
Page: 4257-4267

Journal of Creative Power and Ambition (JCPA)
https://edujavare.com/index.php/jcpa
E-ISSN: 3031-4054
DOI: 10.70610/jcpa.2262

Artificial Intelligence in Auditing and Financial Accounting: Implications for Information Reliability, Accountability, and Investor Trust

Al Putri Oktavia, Nurhayanti, Liza Ulfiana
[1]Politeknik Negeri Sriwijaya, Indonesia;
[2,3] Universitas Islam Al-Kifayah Riau, Indonesia
e-mail: alputrioktavia@polsri.ac.id,, nurhayanti1215@gmail.com; lizaulfiana18@gmail.com

Article history Submitted: 2026/11/05; Revised: 2026/11/09; Accepted: 2026/11/12

Abstract

This article examines how Artificial Intelligence (AI) affects auditing and financial accounting, with particular attention to information reliability, accountability, and investor trust. Using a conceptual literature review, the study synthesizes research on AI-enabled audit analytics, machine learning, robotic process automation, natural language processing, governance, and professional judgment. The analysis indicates that AI can improve the timeliness, consistency, coverage, and analytical depth of accounting and audit procedures by processing large datasets, identifying anomalies, supporting reconciliations, and assisting risk assessment. However, these benefits do not automatically guarantee reliable reporting. Data quality, model bias, limited explainability, cyber risk, automation bias, and weak controls may create new forms of error and uncertainty. Accountability therefore requires clear responsibility for data, model design, validation, human review, documentation, and escalation of exceptions. Investor trust is most likely to be strengthened when AI use is transparent, appropriately governed, independently evaluated, and accompanied by credible assurance and disclosure. The article proposes an integrated framework connecting AI capability, governance controls, information quality, accountability, and investor trust. It concludes that AI should augment—not replace—professional scepticism and judgment, while organizations should establish risk-based governance throughout the AI lifecycle.

Keywords Artificial Intelligence; auditing; financial accounting; information reliability; accountability; investor trust.

© 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution 4.0 International (CC BY SA) license, https://creativecommons.org/licenses/by-sa/4.0/.

INTRODUCTION

Artificial Intelligence (AI) is reshaping the production, examination, and communication of financial information. Technologies such as machine learning, natural language processing, robotic process automation, and generative AI can process transactions at scale, classify documents, identify unusual patterns, support estimates, and produce analytical summaries. In financial accounting, these capabilities may accelerate reconciliations, journal-entry reviews, consolidation, forecasting, and the preparation of management reports. In auditing, AI-enabled analytics can help auditors examine entire populations rather than relying exclusively on samples, prioritize high-risk transactions, and identify relationships that may not be apparent through conventional procedures (Appelbaum et al., 2017; Cao et al., 2015; Kokina & Davenport, 2017).

Nevertheless, the use of AI creates a dual challenge. On the one hand, automation and advanced analytics can improve the speed, consistency, and breadth of accounting and audit work. On the other hand, the reliability of outputs depends on the quality and representativeness of input data, the suitability of models, the design of controls, and the competence of the people who interpret results. An algorithm may generate a precise-looking output while reproducing incomplete records, biased assumptions, or errors embedded in source systems. The use of complex or opaque models may also make it difficult for users and auditors to understand why a particular result was produced (Sutton et al., 2016; Moll & Yigitbasioglu, 2019).

These issues are consequential because financial statements are used by investors, creditors, regulators, and other stakeholders to assess performance, financial position, cash flows, and stewardship. The usefulness of accounting information depends on fundamental qualitative characteristics, particularly relevance and faithful representation, supported by comparability, verifiability, timeliness, and understandability (IFRS Foundation, 2018). If AI improves processing speed but weakens traceability or introduces unrecognized model risk, the apparent efficiency gain may not translate into higher information quality. Accordingly, AI adoption must be assessed not only as a technological investment but also as a governance and accountability issue.

Auditing has a related responsibility. Auditors must obtain sufficient appropriate audit evidence, exercise professional scepticism, and evaluate whether the evidence supports the conclusions reached. Data analytics can strengthen risk assessment and substantive procedures, but an AI-generated alert is not, by itself,

proof of fraud or misstatement. Auditors need to understand the purpose, limitations, data dependencies, and reliability of the tools they use, and must determine whether the procedures provide appropriate evidence (IAASB, 2020; AICPA, 2023). Human judgment remains essential when interpreting anomalies, evaluating estimates, assessing management bias, and communicating significant findings.

Although prior studies have examined automation, audit analytics, and the changing role of accountants, the relationship among AI-enabled processes, information reliability, organizational accountability, and investor trust requires an integrated discussion. This article addresses that need by asking: (1) through what mechanisms can AI affect the reliability of accounting information and audit evidence; (2) what governance and accountability arrangements are necessary to manage AI-related risks; and (3) under what conditions can AI-supported accounting and auditing strengthen investor trust? The article develops a conceptual framework and practical implications for companies, auditors, regulators, and investors.

METHODS

This study uses a conceptual literature review to synthesize academic and institutional publications concerning AI in auditing and financial accounting. The review focuses on five connected areas: (1) AI applications in accounting and auditing; (2) qualitative characteristics and reliability of financial information; (3) audit evidence and professional judgment; (4) AI governance, internal control, and accountability; and (5) investor trust and disclosure. Foundational research on audit analytics and accounting information systems is considered alongside professional and regulatory guidance, including the Conceptual Framework for Financial Reporting, the International Standards on Auditing, the NIST AI Risk Management Framework, and OECD AI principles.

Dimension	Core mechanisms	Implications
AI capability	Automation, machine learning, NLP, predictive analytics, generative AI	Efficiency, broader coverage, faster analysis
Information reliability	Data quality, model validity, explainability, traceability	Timeliness, consistency, faithful representation, verifiability
Accountability	Ownership, validation, human review,	Clear responsibility and defensible professional judgments

	documentation, monitoring	
Investor trust	Transparency, internal control, independent assurance	Confidence in the credibility of reported information

FINDINGS AND DISCUSSION

The literature synthesis indicates that AI affects financial accounting and auditing through four interdependent pathways: process automation, expanded analytical capacity, changes in evidence evaluation, and new governance demands. These pathways can improve information quality, but their effects depend on the controls surrounding data, models, users, and reporting processes. The discussion is organized around the article's three central outcomes: information reliability, accountability, and investor trust.

1. AI Applications in Auditing and Financial Accounting

In financial accounting, robotic process automation can perform repetitive, rule-based activities such as extracting invoice data, matching purchase orders, reconciling accounts, and transferring approved information between systems. Machine-learning tools can assist classification, anomaly detection, and forecasting, while natural language processing can extract information from contracts, invoices, board materials, and other unstructured documents. These applications may reduce manual processing time and support more frequent reporting. They are most effective when processes are standardized, source data are controlled, and exceptions are routed to qualified personnel (Kokina & Davenport, 2017; Moll & Yigitbasioglu, 2019).

In auditing, data analytics and machine-learning techniques can support risk assessment, journal-entry testing, fraud-risk procedures, and the examination of large transaction populations. Pattern recognition can identify unusual timing, amounts, counterparties, or combinations of attributes. Text analytics may help auditors review large volumes of contracts and disclosures. Earlier research on continuous auditing and audit data analytics emphasizes the potential to move from periodic, sample-oriented procedures toward more continuous and risk-focused analysis (Alles, 2015; Appelbaum et al., 2017; Gepp et al., 2018).

However, AI does not eliminate the need to define an audit objective and design an appropriate procedure. A model trained to identify unusual transactions may miss a new fraud pattern that differs from its training data, or may flag legitimate transactions as suspicious. The auditor must assess whether the population is

complete, whether the model is appropriate for the assertion being tested, and whether the output can be corroborated with other evidence. AI should therefore be treated as an instrument within the audit methodology rather than as an autonomous decision-maker (Brown-Liburd et al., 2015; Earley, 2015).

2. Implications for the Reliability of Financial Information

Information reliability is strengthened when accounting information faithfully represents the economic phenomena it purports to represent. AI can contribute by applying consistent processing rules, reducing certain forms of manual error, reconciling records more frequently, and identifying anomalies before financial statements are finalized. Wider analytical coverage can also improve the likelihood that unusual transactions or inconsistencies are investigated. These benefits support timeliness and verifiability when the underlying process is appropriately documented and controlled (IFRS Foundation, 2018; Cao et al., 2015).

Yet automation can also scale errors. Inaccurate master data, missing transactions, inconsistent labels, or biased training samples can lead to systematically misleading outputs. Model drift may reduce performance when business conditions change, while data leakage or inappropriate feature selection can create an illusion of predictive accuracy. Generative AI introduces additional concerns, including fabricated references, unsupported explanations, and outputs that sound authoritative despite being incorrect. Accordingly, organizations should establish data lineage, validation rules, version control, periodic performance testing, and clear procedures for correcting errors.

Explainability is particularly important in financial reporting. When an AI system influences a material estimate, classification, impairment assessment, or risk judgment, responsible personnel should be able to explain the relevant inputs, assumptions, model limitations, and human decisions. Explainability does not require every model to be mathematically simple; it requires a level of transparency proportionate to the significance of the decision and the risks to users. The NIST AI Risk Management Framework highlights governance, mapping, measurement, and management as connected functions for managing AI risks throughout the system lifecycle (NIST, 2023).

Table 1. AI Applications and Their Implications for Information Reliability

Application | Potential contribution | Principal reliability risk | Key control response

Transaction processing and reconciliation | Faster, more consistent processing | Incorrect source data or rule configuration | Input validation, reconciliations, exception review

Anomaly and fraud analytics | Broader identification of unusual patterns | False positives, false negatives, model drift | Model validation, threshold testing, corroborating evidence
Document and contract analysis | Faster extraction of relevant terms | Misclassification or omitted clauses | Human verification, sampling, source-document traceability
Forecasting and estimates | More timely scenario analysis | Biased assumptions and opaque outputs | Independent challenge, sensitivity analysis, approval controls
Generative AI assistance | Drafting and summarization efficiency | Hallucinations, confidentiality leakage | Approved tools, restricted data, fact-checking, disclosure

Source: Authors' synthesis of the literature.

3. Accountability, Internal Control, and Professional Responsibility

AI adoption can distribute decisions across data owners, software vendors, model developers, system administrators, finance personnel, internal auditors, and external auditors. Without explicit role allocation, responsibility may become fragmented: users may rely on vendor assurances, managers may assume that technical teams have validated outputs, and auditors may misunderstand the limits of automated procedures. Accountability requires an identifiable owner for each material AI use case and a documented chain of responsibility from data acquisition to final reporting.

At the organizational level, governance should cover approval before deployment, classification of use cases by risk, access control, data protection, model validation, monitoring, change management, incident response, and retirement of systems that no longer perform as intended. These arrangements should be integrated with internal control over financial reporting rather than operated as a separate technology checklist. The COSO internal control framework provides a basis for considering control environment, risk assessment, control activities, information and communication, and monitoring in relation to AI-enabled processes (COSO, 2013).

At the professional level, accountants and auditors remain responsible for the conclusions they make, even when AI tools assist their work. They should understand the tool sufficiently to evaluate its relevance and limitations, maintain professional competence, protect confidential information, and apply professional scepticism. The use of an AI system cannot transfer ethical or professional responsibility to the algorithm or its provider. Where an output materially affects a financial statement assertion or audit conclusion, the responsible professional should

document the tool's purpose, data used, procedures performed, exceptions identified, human review, and final rationale (IAASB, 2020; AICPA, 2023).

The governance challenge also extends to third-party systems. Organizations should evaluate vendor access to confidential information, data retention, subcontracting, cybersecurity, model updates, service continuity, and the ability to obtain relevant documentation. Contracts and service-level arrangements should clarify responsibilities for security incidents, system changes, and audit access. A risk-based approach is consistent with the OECD principles that emphasize transparency, robustness, security, and accountability in trustworthy AI (OECD, 2019).

4. AI and Investor Trust

Investor trust depends on whether financial information is credible, comparable, timely, and supported by effective governance and assurance. AI may strengthen trust when it improves the consistency of reporting, supports earlier detection of irregularities, and enables auditors to examine more extensive datasets. More timely identification of errors can reduce information asymmetry and help investors assess management performance and financial risk. However, technology adoption alone is not a signal of trustworthy reporting.

Trust may be weakened when companies provide little information about material AI use, when model outputs cannot be explained, or when automated processes create errors that are difficult to detect. Investors may also question whether management has used AI to produce optimistic forecasts, manipulate assumptions, or obscure uncertainty. Consequently, disclosures should be proportionate to materiality and explain the role of AI in significant reporting processes, the governance arrangements in place, important limitations, and the nature of human oversight. Disclosure should not expose proprietary information unnecessarily, but it should provide enough context for users to understand how material judgments are made.

Independent assurance is another important trust mechanism. External auditors do not certify that an organization's AI is universally accurate; they obtain evidence relevant to the financial statements and evaluate the controls and procedures that affect audit risk. When AI tools are used by management or auditors, the reliability of those tools and their outputs should be considered within the relevant audit approach. Investors are more likely to place confidence in AI-enabled reporting when technology is accompanied by robust internal controls, transparent governance, competent professionals, and credible independent assurance (Moffitt et

al., 2018; Sutton et al., 2016).

5. An Integrated Conceptual Framework

The literature supports a framework in which AI capability influences information reliability through the quality of data, model performance, process integration, and the extent of analytical coverage. Governance and accountability act as enabling and moderating conditions: they determine whether AI outputs are validated, traceable, secure, and subject to appropriate human review. Improved information reliability and credible assurance can then contribute to investor trust, while failures in governance can weaken or reverse the expected benefits.

Table 2. Integrated Framework Linking AI, Reliability, Accountability, and Investor Trust

AI capabilities | Governance and accountability conditions | Information and assurance outcomes | Expected investor response

Automation, machine learning, NLP, predictive analytics | Data ownership, access controls, model validation, documentation, human review | More timely processing, broader analysis, traceable evidence | Greater confidence when outputs are credible and explainable

Generative AI and decision support | Approved use cases, confidentiality safeguards, fact-checking, escalation rules | More efficient drafting and analysis, subject to verification | Trust depends on transparent limits and responsible use

Continuous monitoring and anomaly detection | Ongoing performance monitoring, independent review, incident management | Earlier identification of exceptions and control weaknesses | Stronger confidence when issues are investigated and resolved

Source: Authors' conceptual synthesis.

The framework suggests three propositions. First, AI capability is more likely to improve information reliability when input data are complete, models are fit for purpose, and outputs are subject to validation. Second, clear accountability and effective internal controls strengthen the relationship between AI use and reliable reporting by ensuring that responsibility, review, and documentation remain identifiable. Third, the effect of AI-enabled reporting on investor trust is mediated by perceived information quality and credible assurance; adoption without transparency or control may have little positive effect and may damage confidence.

6. Practical Implications for Organizations, Auditors, and Regulators

For companies, AI implementation should begin with a documented business and reporting objective rather than technology adoption for its own sake. Management should maintain an inventory of AI systems used in material accounting processes,

classify them according to financial reporting risk, assign accountable owners, and define approval and monitoring requirements. High-impact systems should undergo independent validation before deployment and after significant changes. Staff training should cover data quality, model limitations, cybersecurity, confidentiality, and the appropriate challenge of automated outputs.

For audit firms, methodologies should specify when AI-assisted procedures are appropriate, what evidence is required to support reliance on tool outputs, and how exceptions are investigated. Engagement teams need access to personnel with data and technology expertise, but responsibility for audit judgments must remain with the engagement team. Audit documentation should enable an experienced auditor to understand the procedures, relevant data, tool limitations, results, and judgments made. Professional bodies and educators should also strengthen training in data analytics, AI governance, ethics, and critical evaluation.

For regulators and standard setters, guidance should encourage innovation while clarifying expectations for governance, transparency, documentation, cybersecurity, and human oversight. Requirements should be proportionate to the materiality and risk of each application. The objective should not be to prescribe a single technology but to ensure that the use of AI does not undermine established principles of faithful representation, audit quality, accountability, and investor protection.

7. Limitations and Future Research

This article is a conceptual literature review and does not report primary interviews, surveys, experiments, or archival tests. Its conclusions therefore represent a synthesis of prior research and professional frameworks rather than empirical estimates of the effect of AI on reporting quality or investor behavior. The pace of technological development also means that specific tools and regulatory expectations may change. Future research could test the proposed framework using company-level data, auditor surveys, investor experiments, or case studies of AI implementation. Further work is also needed to compare the effects of different AI applications, assess the cost of governance controls, and examine how disclosure practices influence investor judgments across industries and regulatory environments.

CONCLUSION

This article concludes that AI can improve auditing and financial accounting by accelerating routine processes, expanding analytical coverage, and supporting the identification of unusual transactions and reporting risks. These capabilities can

contribute to more timely, consistent, and verifiable information, but they do not automatically ensure reliability. Data defects, model bias, limited explainability, cybersecurity threats, and overreliance on automated outputs can undermine the quality of financial reporting and audit evidence. Organizations therefore need lifecycle governance, clear data and model ownership, validation, documentation, access controls, monitoring, and meaningful human review. Accountants and auditors remain accountable for their professional judgments and must apply scepticism when interpreting AI-generated outputs. Investor trust is most likely to improve when AI-enabled processes are transparent, well controlled, supported by competent professionals, and subject to credible independent assurance. AI should consequently be understood as an augmentation of professional capability rather than a substitute for accountability, ethics, or judgment.

REFERENCES (Palatino Linotype 12, Single Space, Justify, Mendelay, Endnote, APA (American Psychological Association) Style and the 7th edition)

Alles, M. G. (2015). Drivers of the use and facilitators and obstacles of the evolution of big data by the audit profession. Accounting Horizons, 29(2), 439–449. https://doi.org/10.2308/acch-51067

American Institute of Certified Public Accountants. (2023). Audit evidence: A guide to applying audit data analytics. AICPA.

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement: Research needs. Auditing: A Journal of Practice & Theory, 36(4), 1–27. https://doi.org/10.2308/ajpt-51684

Brown-Liburd, H., Issa, H., & Lombardi, D. (2015). Behavioral implications of Big Data's impact on audit judgment and decision making and future research directions. Accounting Horizons, 29(2), 451–468. https://doi.org/10.2308/acch-510(bigdata)

Cao, M., Chychyla, R., & Stewart, T. (2015). Big data analytics in financial statement audits. Accounting Horizons, 29(2), 423–429. https://doi.org/10.2308/acch-51068

Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal control—Integrated framework. COSO.

Earley, C. E. (2015). Data analytics in auditing: Opportunities and challenges. Business Horizons, 58(5), 493–500. https://doi.org/10.1016/j.bushor.2015.05.002

Gepp, A., Linnenluecke, M. K., O'Neill, T. J., & Smith, T. (2018). Big data techniques in auditing research and practice: Current trends and future opportunities. Journal of Accounting Literature, 40, 102–115. https://doi.org/10.1016/j.acclit.2017.05.003

International Auditing and Assurance Standards Board. (2020). Non-authoritative support material: The use of technology in the audit of financial statements. International Federation of Accountants.

IFRS Foundation. (2018). Conceptual framework for financial reporting. IFRS Foundation.

Institute of Internal Auditors. (2024). Artificial intelligence: Considerations for the internal audit profession. The Institute of Internal Auditors.

Issa, H., Sun, T., & Vasarhelyi, M. A. (2016). Research ideas for artificial intelligence in auditing: The formalization of audit and workforce supplementation. Journal of Emerging Technologies in Accounting, 13(2), 1–20. https://doi.org/10.2308/jeta-10511

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

Moffitt, K. C., Rozario, A. M., & Vasarhelyi, M. A. (2018). Robotic process automation for auditing. Journal of Emerging Technologies in Accounting, 15(1), 1–10. https://doi.org/10.2308/jeta-10589

Moll, J., & Yigitbasioglu, O. (2019). The role of internet-related technologies in shaping the work of accountants: New directions for accounting research. The British Accounting Review, 51(6), 100833. https://doi.org/10.1016/j.bar.2019.04.002

National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

Organisation for Economic Co-operation and Development. (2019). Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). OECD.

Sutton, S. G., Holt, M., & Arnold, V. (2016). The reports of my death are greatly exaggerated—Artificial intelligence research in accounting. International Journal of Accounting Information Systems, 22, 60–73. https://doi.org/10.1016/j.accinf.2016.07.005

Vasarhelyi, M. A., Kogan, A., & Tuttle, B. M. (2015). Big data in accounting: An overview. Accounting Horizons, 29(2), 381–396. https://doi.org/10.2308/acch-51071

Zhang, C. (2019). Intelligent process automation in audit. Journal of Emerging Technologies in Accounting, 16(2), 69–88.