Communication in Physical Sciences, 2024, 11(4) :1235-1249

Assessing Transparency and Accountability Mechanisms in AI-Driven Audit Tools

Olatunde Ayeomoni, Sugar Raymond and Jude Okwuchukwu Ogene
Received: 28 August 2024/Accepted: 18 December 2024/Published:31 December 2024

Abstract: *The current paper looks at transparency and accountability features integrated into the artificial intelligence-driven audit tools with critical concerns regarding the algorithmic decision-making in the financial and regulatory oversight settings. A mixed-methods methodology that involves technical examination of fifteen popular audit systems, semi-structured interviews with sixty professionals in various stakeholder groups, and three detailed case studies, will enable us to methodically evaluate how modern AI audit systems apply explainability functionality, provide decision-making log trails, and create accountability systems. We find that transparency practices strongly vary across the various categories of tools, as commercial platforms show moderate adoption of explainable AI capabilities but accountability mechanisms are largely procedural and not technical. We outline problematic aspects of existing implementations, such as limited stakeholder access to algorithmic decision-making, a lack of algorithmic decision process provenance and model validation processes documentation, and inadequate interaction with existing regulatory frameworks for the audit practice. The research suggests a multi-dimensional framework of evaluation of transparency and accountability of AI audit tools, which is a consolidation of technical, procedural, organization, and regulatory factors. We provide evidence-based recommendations to developers, audit practitioners, and regulators to enhance trustworthiness and performance of AI-driven audit systems while addressing inherent trade-offs between transparency, competitiveness, and system complexity.*

Keywords*: Artificial Intelligence, Audit Technology, Transparency, Accountability, Explainable AI, Algorithmic Governance, Financial Technology, Regulatory Compliance, etc.*

Olatunde Ayeomoni
University of Cincinnati, School of Information Technology, Cincinnati, Ohio, USA.
Email: ayeomooe@mail.uc.edu

Sugar Raymond
University of Cincinnati, School of Information Technology, Cincinnati, Ohio, USA.
Email: Sugarraymond@gmail.com

Jude Okwuchukwu Ogene
Kennesaw State University, College of Computing and Software Engineering, Marietta, Georgia, USA.
Email: Joption7@gmail.com

1.0 Introduction

The incorporation of artificial intelligence into audit procedures has fundamentally changed the nature of financial and compliance oversight moving what has always been a labour-intensive and judgment-driven practice to a more automated and data-intensive one. “Modern AI-driven audit tools now perform risk analysis, detect anomalies, generate preliminary findings, and even draft sections of audit reports at scales and speeds previously unimaginable (Kokina and Davenport, 2017). The largest accounting companies have spent billions on their own AI systems, including Clara by KPMG, Argus by Deloitte, GL.ai by PwC, and Canvas Analytics by EY are only a few examples of this technological change (Brown-Liburd *et al*., 2015). These systems can analyze millions of transactions in hours, see patterns that a human auditor can miss and mark out anomalies with more sophisticated algorithms. “However, this rapid adoption has outpaced critical consideration of a central issue: how can

systems whose decision-making processes are often opaque to users be trusted, certified, and effectively supervised by auditors, regulators, and audited entities?"

These challenges are not merely technical; they directly concern the social role of auditing, which is the issue of the opacity of AI audit tools. The value of auditing lies not only in detecting errors or fraud but in providing assurance grounded in transparency, reproducibility, and the ability to critically evaluate audit findings (Power, 1997). This is the distinguishing feature of audit as opposed to mechanical checking. In the case when an AI system sends an alert about a potentially fraudulent transaction or the system rates a specific account as highly risky, the stakeholders cannot afford a binary response; they seek to know the reasoning behind a certain decision, the pattern of data it identified, the confidence rates of a specific conclusion, the assumptions that the system made (Areghan, 2023; Dwork *et al*., 2012). Without such transparency, AI-based audits risk becoming mechanical compliance tools rather than instruments of critical financial assurance. The lack of transparency directly intersects with accountability structures in audit practice. The accountability built into traditional audit methodology has many layers: documentation requirements help to ensure that audit procedures and findings are subject to review and validation; professional standards provide benchmarks on the quality of work in an audit; a peer review process is a way to ensure that the work is validated by an external body; and the last form of accountability is the legal liability in case of audit failure, which creates powerful incentive in the way of diligence (DeFond and Zhang, 2014). However, when large amounts of audit work are left to algorithmic systems these accountability mechanisms are confronted with new challenges. When an AI system fails to detect a material misstatement, responsibility becomes unclear. Should accountability rest with the algorithm developer, the audit firm that deployed the system, the individual auditor, or the organization that configured its parameters? Existing legal and professional frameworks provide limited guidance, creating uncertainty in liability allocation and standards of professional responsibility (Kroll *et al*., 2017; Onwuegbuchi *et al*., 2023). These concerns extend beyond individual audit engagements. AI audit tools find more and more applications not only in financial auditing but in regulatory compliance, internal controls audit, fraud audit, environmental sustainability reporting, and even social responsibility audit (Aboagye *et al*., 2022). The impact of the opaque systems is magnified as this becomes increasingly embedded in the systems of corporate governance and regulatory infrastructure. Corrupted training data, an over-fit model, or incorrectly tuned confidence metric may cause risk measurements to be systematically biased across thousands of organizations, and introduce systematic vulnerabilities that cannot be monitored by human control (Adeyemi, 2023). The risk of cascading failures is particularly high when multiple organizations rely on similar AI systems trained on shared or correlated datasets. which may cause errors that are correlated and may increase, instead of diversifying, the risk. In the meantime, the competition situation in the audit technology market can in fact subvert transparency, since vendors treat their algorithms as a competitive intellectual property that needs protection against the rivalry (Burrell, 2016). This is a troubling paradox it is those very features that have rendered AI audit tools so useful like their ability to recognize patterns and process data in a sophisticated way that relies on complex algorithms, which are not easily explained.

Despite growing interest, the literature on transparency and accountability in AI-driven audit tools remains fragmented across disciplines. Scholars in the field of computer science have developed more elaborate methods of model interpretability, such as local interpretable model-agnostic explanations (LIME), Shapley additive explanations (SHAP), and attention

mechanisms of deep learning (Ribeiro *et al*., 2016; Lundberg and Lee, 2017). Yet, such approaches are frequently constructed to address generic classification issues as opposed to the particularities of audit situations, where professional standards and regulatory and liability issues pose unique challenges. In the meantime, auditing research has studied the adoption patterns and user acceptance and selected factors that affect the willingness of auditors to use AI tools and the availability of organizational resources to implement AI (Issa *et al*., 2016; Munoko *et al*., 2020). Nonetheless, this literature tends to discuss transparency as a dichotomous notion, i.e. it is or it is not but does not focus on its multi-dimensional nature. The regulatory scholarship recognizes the governance implications of algorithmic systems (Coglianese and Lehr, 2017) but is seldom concerned with the technical aspects of the implementation of the audit tools. What is still lacking is a systematic empirical evaluation of how transparency and accountability mechanisms are implemented in real-world AI audit tools and how these implementations align with stakeholder expectations. This study addresses this gap by empirically evaluating transparency and accountability mechanisms in AI-driven audit tools using technical analysis, stakeholder interviews, and case studies. In this study, transparency is conceptualized as a multidimensional construct comprising technical, process, and outcome transparency. in model architecture and decision logic, process transparency in development and validation methodology, and outcome transparency in explanation of particular decisions (Diakopoulos, 2016; Kemper & Kolkman, 2019). This multi-dimensional conceptualization acknowledges that various parties might need the transparency of various forms, regulators might focus on the process transparency to confirm the adherence to the standards, and auditors may focus on the outcome transparency to confirm the correctness of particular decisions. Similarly, accountability is conceptualized as encompassing technical, procedural, and organizational dimensions. (Dwork & Mulligan, 2013). This is a holistic approach that recognizes that accountability cannot be brought about by technical means but organizational and professional commitment is a necessary requirement.

The objectives of this study are to:

(i) Systematically assess existing transparency and accountability mechanisms in AI-driven audit tools
(ii) Evaluate their adequacy in meeting stakeholder needs
(iii) Identify gaps between current implementations and expected standards
(iv) Develop a structured evaluation framework for transparency and accountability in audit AI systems

This study is significant because AI adoption in auditing is accelerating faster than the development of governance and accountability mechanisms. The findings will support auditors, developers, regulators, and policymakers in designing more transparent and trustworthy AI audit systems. It also contributes to improving audit reliability in increasingly automated financial environments.

The paper has continued with an analysis using a theoretical framework, description of methodology, presentation of results, discussion of findings, and recommendations to developers, practitioners, and regulators.

1.1 Theoretical Framework

Multiple intellectual traditions inform the theoretical foundation of transparency and accountability in AI-driven audit tools, since these concepts operate across technical, organizational, and regulatory dimensions.

1.1.1 Algorithmic System Transparency

Transparency in AI systems has been conceptualized at multiple levels, each addressing different dimensions of system understanding and verification. At the foundational level, technical transparency refers to the extent to which the internal functioning of an AI model can be understood and examined (Lipton, 2018). It includes model interpretability, i.e., how well humans

are able to understand the reasons why a model generates specific output, and model inspectability, i.e., whether it is possible to inspect the model components, parameters, and decision logic (Adabi Berrada, 2018). Technical transparency is however a graded property and not a binary one.“Linear regression models are inherently interpretable because the contribution of each input variable to the output can be directly quantified. Decision trees also allow visual representations of decision logic which can be followed using a series of sequential branching rules. In contrast, deep neural networks containing millions of parameters distributed across multiple hidden layers often require post-hoc interpretability techniques such as LIME and SHAP to approximate their decision logic (Ribeiro *et al*., 2016; Lundberg & Lee, 2017). These methods generate simplified, interpretable approximations of complex model behavior within localized regions of the input space. Beyond technical transparency, process transparency concerns the procedures involved in model development, validation, and deployment (Diakopoulos, 2016). This includes documentation of training data sources, preprocessing procedures, validation methods, and deployment conditions. A model that was developed using historical data of one industry or time might not work well when used in another context. Process transparency is also about the revelation of validation methodologies and performance metrics, not only the overall accuracy, but also performance on various subgroups, false positive and false negative rates, and sensitivity to perturbations. It also requires clarification of operational conditions under which the model is expected to function reliably and situations where human oversight becomes necessary. Process transparency is particularly important in auditing because the credibility of audit conclusions depends not only on correctness but also on adherence to professional standards and evidence-gathering procedures. (Okolo, 2023). Not only should the opinion of the audit be defensible according to its correctness, but also according to the use of the professionally required standards, due care, and the appropriate use of the evidence collection procedures.Outcome transparency focuses on explaining specific model decisions or predictions (Selbst and Barocas, 2018). In the case of AI audit tools, this should include giving the stakeholders explainable reports of why certain transactions have been identified as suspicious, why some risk assessment was created or how some audit conclusions were drawn. Effective explanations should identify the features or patterns influencing a decision, provide confidence estimates, compare outcomes with historical examples, and indicate alternative conditions that could have produced different results. Most importantly, outcome explanations should be tailored to the knowledge level and informational needs of different stakeholders. Data scientists may prefer technical explanations involving feature attribution and model internals, whereas audit clients may require simplified and business-oriented explanations. Conversely, overly simplified explanations may be insufficient for regulators seeking to assess compliance with professional audit standards (Sokol & Flach, 2020). Despite its importance, transparency has practical and technical limitations. that can be overcome by technical means only. Full transparency can be technically impossible with complex models in which even the creators of the model do not know how particular decisions arise as a result of interactions between thousands or millions of parameters. From a commercial perspective, extensive disclosure may threaten proprietary intellectual property and competitive advantage. Excessive technical detail may also overwhelm users, resulting in information overload and reduced interpretability. “Excessive technical detail may also overwhelm users, resulting in information overload and reduced interpretability (Burrell, 2016). Consequently, Ctransparency involves unavoidable trade-offs that require balancing stakeholder needs, technical feasibility, and

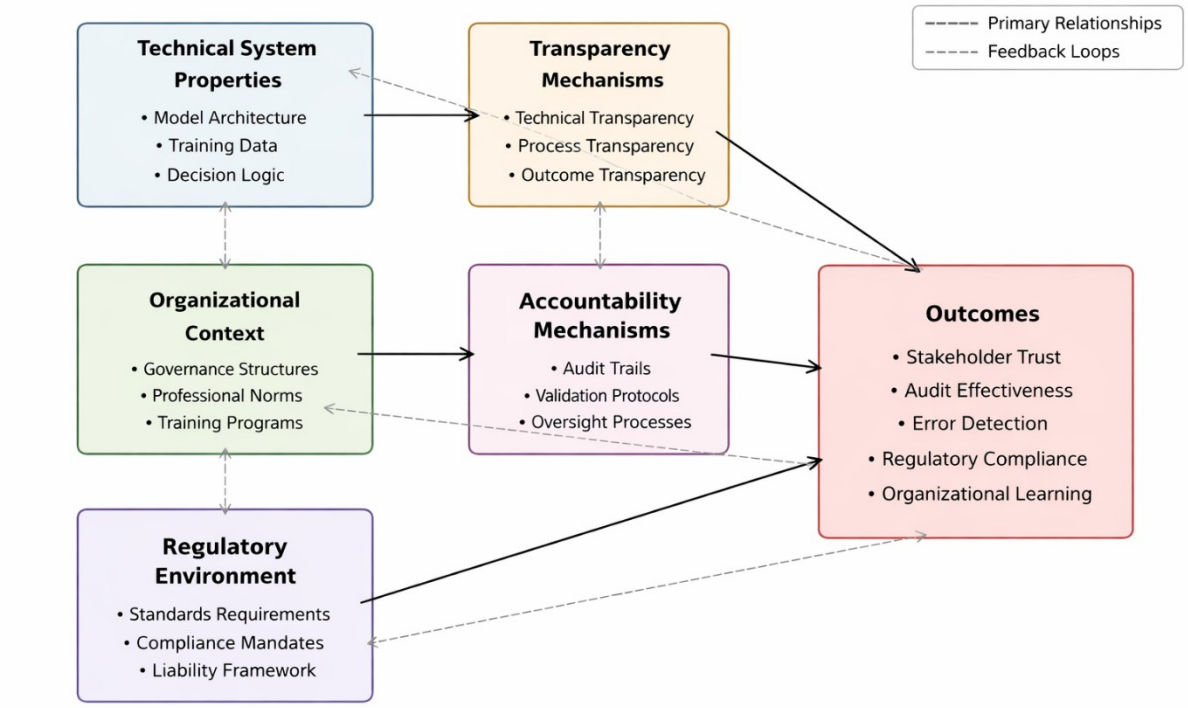
organizational interests (Ananny & Crawford, 2018). In addition to transparency, accountability has emerged as a critical governance principle in AI-enabled auditing systems.

1.1.2 Accountability and Responsibility in AI Systems

Accountability in AI systems extends beyond the simple attribution of responsibility. Drawing on Bovens (2007), accountability is conceptualized as involving three essential elements: an accountable actor, a forum to which explanations are provided, and a process through which actions are evaluated. In the context of AI audit tools, this framework becomes complicated because multiple agents are often involved. Technical accountability mechanisms are developed with characteristics that allow to remake systems behavior and verifying it. Audit trails that record inputs, intermediate processes, and outputs enable retrospective analysis of system behavior.

Version control systems record the changes to models and configurations over time. Data lineage records the movement of the information in processing pipelines (Passi & Barocas, 2019).

Procedural accountability involves governance mechanisms that regulate AI system development, deployment, and monitoring. This involves validation procedures that measure the performance of the models prior to deployment, observing mechanisms that identify degradation, and controls that will review the outcomes that resulted in human reviews (Amoore & Raley, 2017). Legal and regulatory frameworks further establish formal responsibility structures for AI-related audit outcomes. However, accountability mechanisms for AI-driven audit outcomes remain underdeveloped in current audit practice (Coglianese & Lehr, 2017).



Conceptual framework illustrating relationships between AI system properties, transparency mechanisms, contextual factors, and audit outcome."

Fig. 1: Conceptual model that shows the connections among the properties of AI systems, transparency and accountability systems, situational conditions, and audit findings.

1.1.2 Trust and Legitimacy

Transparency and accountability play both instrumental and symbolic roles in building trust and legitimacy in AI-enabled auditing systems. (Ranerup & Zinner Henriksen, 2019). Trust in auditing includes competence trust, which reflects confidence in technical capability, and integrity trust, which reflects belief in ethical and professional conduct (DeFond & Zhang, 2014). Trust in auditing includes competence trust, which reflects confidence in technical capability, and integrity trust, which reflects belief in ethical and professional conduct (DeFond & Zhang, 2014). Legitimacy is strengthened when audit processes conform to accepted procedural and professional norms (Suchman, 1995). The use of AI tools where there is no transparency can jeopardize the perceived legitimacy despite any technical superiority (Power, 1997).

1.2 Conceptual Model

Fig. 1 presents the conceptual framework guiding this study. The framework illustrates how transparency and accountability emerge through interactions among technological, organizational, professional, and regulatory factors. The framework highlights that complex interactions of technology, organization, profession and regulation are what bring transparency and accountability.

2.0 Method

2.1 Research Design

This study adopted a convergent mixed-methods approach that combined quantitative technical evaluation, qualitative stakeholder interviews, and case study analysis (Creswell and Plano Clark, 2018)."

This method acknowledges that the issue of transparency and accountability cannot be effectively assessed using one particular methodology. Methodological triangulation enhanced the reliability and depth of the findings.

2.2 Sample Selection

Fifteen AI-driven audit tools representing different market segments were purposively selected for analysis. Selection criteria included commercial availability, application of machine learning techniques, relevance to financial auditing or compliance evaluation, and willingness of vendors or organizations to participate.

The sample consisted of eight commercial platforms, three open-source tools, and four proprietary enterprise systems. Table 1 indicates the features of tools in our sample.

Table 1: Characteristics of AI Audit Tools in Sample

Tool Category	Number	Primary Function	AI Techniques	Target Users
Commercial Platform A	3	Fraud Detection	Neural Networks, Clustering	Audit Firms
Commercial Platform B	3	Risk Assessment	Random Forests, NLP	Corporations
Commercial Platform C	2	Compliance Monitoring	SVM, Anomaly Detection	Regulators
Open-Source Tools	3	General Audit Analytics	Various ML Methods	Academic/Research
Proprietary Enterprise	4	Internal Controls	Ensemble Methods	Large Enterprises

Semi-structured interviews of sixty participants (including audit professionals (n=25), AI developers (n=12), regulatory personnel, (n=8), and audited entity representatives (n=15)) were used. Three organizational case studies were examined,

including: the deployment of AI audit tools in the organizational setting: a financial services company deploying fraud detection software, a local audit firm deploying a commercial analytics technology, and a multinational corporation developing its own AI tools.

2.3 Data Collection and Analysis

Data were collected and analyzed using multiple complementary methods. "Each tool underwent hands-on testing and detailed documentation review. The technical assessment focused on explainability features, documentation quality, audit trail capabilities, training data transparency, and model validation procedures. Semi-structured interviews lasting between 45 and 75 minutes were professionally transcribed for analysis. A multi-dimensional framework that included technical transparency, procedural transparency, technical accountability, and procedural accountability was used in its analysis.

Descriptive statistics were used in analyzing quantitative data. The thematic analysis of qualitative data was performed according to the standard procedures (Braun & Clarke, 2006), and transcripts were coded in NVivo. Patternmatching and explanation-building were the two methods through which case study data were analyzed (Yin, 2018).Research rigor was enhanced through triangulation, participant validation, and detailed contextual description.

3.0 Results and Discussion

3.1 Existing Mechanisms of Transparency\

Technical analysis indicates that AI audit tools are very diverse in terms of their transparency features. Technical analysis revealed substantial variation in transparency features across AI-driven audit tools.

The distribution of the transparency features is provided in Table 2, showing that only six out of the fifteen tools (40%) offer meaningful explainability other than simple reporting of outputs.

Table 2: Transparency Features Across AI Audit Tools (N=15)

Feature Category	Present	Partial	Absent	Sophistication Score
Explainability Interface	6	5	4	2.1 / 5.0
Feature Importance	8	3	4	2.6 / 5.0
Confidence Scores	11	2	2	3.2 / 5.0
Decision Pathways	4	6	5	1.8 / 5.0
Training Data Disclosure	3	4	8	1.4 / 5.0
Model Architecture Details	5	2	8	1.7 / 5.0
Validation Documentation	9	4	2	2.9 / 5.0

As shown in Table 2, confidence scores are the most widely applied transparency feature, and eleven of the tools have this feature. More advanced explainability capabilities, such as decision pathway visualization, were observed in only four tools. and critical information regarding training data sources is mostly not disclosed.

Fig. 2 shows the explainable AI techniques applied in different tools. Post-hoc explainability techniques were the dominant approach, with feature-importance ranking being the most frequently implemented method. in eight out of ten tools which have explainability capabilities. Only three of them use advanced methods such as SHAP, or attention visualization.

Data provided in interviews indicates that the implementation of explainability is a secondary consideration as opposed to design. We built the model to maximize accuracy. Explainability was introduced later when clients began asking questions we could not adequately answer. The explanation was developed much later when clients began to pose questions that we were not able to answer. This reactive approach reflects broader tensions between predictive performance and interpretability in AI system development. Developers have noted that

procurement processes always tend to focus on the accuracy metrics and processing speed, and transparency requirements are often found after the deployment, when users start to face those decisions that cannot be validated or explained to interested people.

The heterogeneity in the quality of documentation is also similar to tools. Commercial vendors generally provide extensive user manuals, tutorials, workflow demonstrations, and troubleshooting documentation. that are more than 100 pages long. However, technical disclosure remained limited.

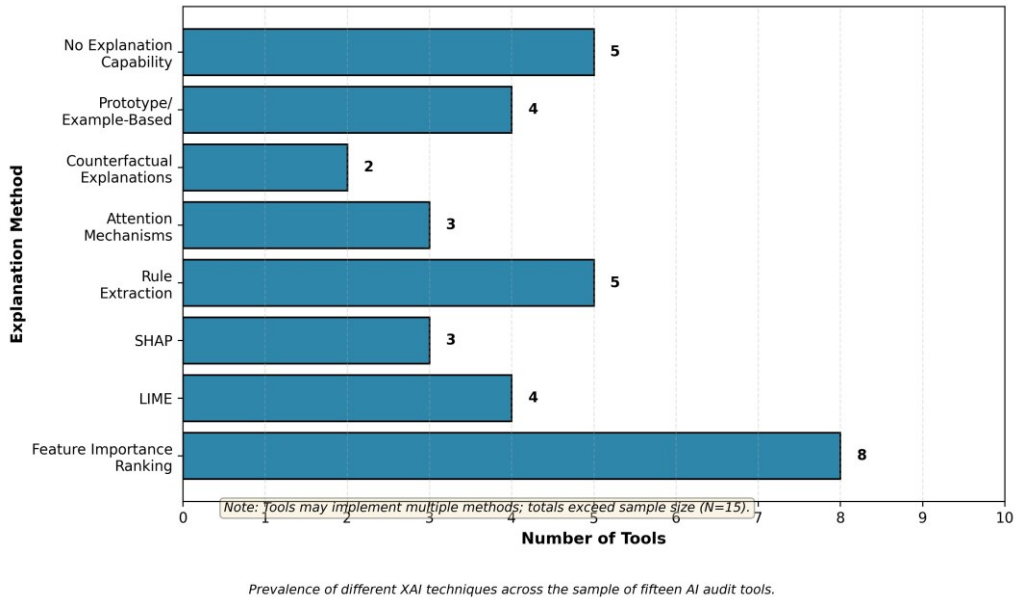


Fig. 2: Prevalence of different XAI techniques across the sample of fifteen AI audit tools.

Only two of the eight commercial tools offer substantial information about model structure beyond an architectural description. Data documentation on training was especially limited, with only three of fifteen tools having anything of significance to say about the source of data, preprocessing, quality checks, or any other known limitations. Limited disclosure of training data provenance raises concerns regarding bias, model applicability, and contextual reliability. (Aboagye *et al*., 2022; Okolo, 2023). Unless they are familiar with training data provenance, auditors will be unable to determine how models apply to their contexts, the situations in which they may perform poorly because of variation between training and deployment conditions.

3.2 3.2 Accountability Mechanisms and Governance Structures

Accountability features provide a little more indication of how they are implemented compared to transparency features, but still contain major gaps. Table 3 summarizes the evaluation of accountability mechanisms.

Table 3: The Audit Trail and Accountability Features Evaluation (N=15)

Feature	Comprehensive	Partial	Minimal	Average Score
Decision Logging	8	5	2	2.8 / 4.0
Data Lineage Tracking	5	4	6	2.1 / 4.0
Model Versioning	9	3	3	2.9 / 4.0
Configuration Logging	7	6	2	2.7 / 4.0
Human Intervention Recording	6	5	4	2.3 / 4.0
Temporal Audit Trail	10	3	2	3.1 / 4.0
Reproducibility Support	4	7	4	2.2 / 4.0

As shown in Table 3, although the majority of tools retain a certain level of decision logging and temporal audit trail, tools with extensive audit trails that allow to recreate the entire decision-making processes are present in less than half. Data lineage tracking, which is essential for understanding data transformation processes, remained relatively weak. Human intervention recording was only partially implemented despite its importance in documenting interactions between professional judgment and algorithmic recommendations. Fig/ 3 shows the common trends in human-AI interaction found in audit processes. Approximately 47% of the tools employed a human-in-the-loop approach in which AI-generated recommendations were subject to human approval, modification, or rejection.

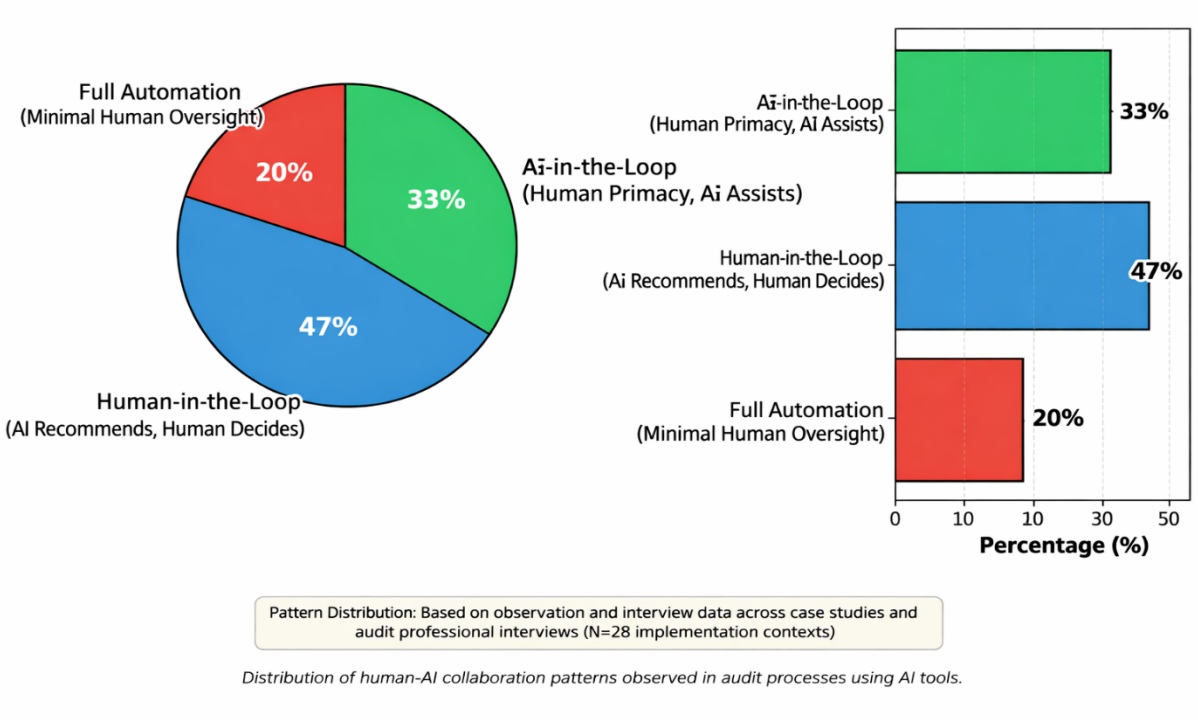


Fig. 3: The distribution of human-AI collaboration patterns that exist in the process of AI-based audits.

As Fig. 3 indicates, the human-in-the-loop arrangements are prevalent, which implies that some awareness of the fact that complete automation poses the issues of professionalism and liability. Nonetheless, evidence provided in the interview shows that the level of human control is quite different. Some implementations provided sufficient contextual information for auditors to critically evaluate AI recommendations, whereas others appeared susceptible to automation bias.

3.3 Stakeholder Perspectives

Thematic analysis revealed significant variation in stakeholder perceptions regarding transparency and accountability priorities.

Table 4 shows the topics of the interviews with auditors. The Table reveals that trust calibration seemed to be the major concern, with 84 percent of auditor respondents referring to it. The theme reflects the challenge of trying to build proper trust, neither blind faith nor automatic scepticism, when model thinking is in the clouds. One of the experienced auditors expounded: I can oversee the work of a junior staff member, inquire and get to know how they think.

Under the AI, I am provided with an answer, but not with how it obtained that answer. It is quite difficult to decide when I need to push

back then. This not openness poses operational problems to auditors who have on themselves to accept AI suggestions, perform further validation, or disregard the system altogether. Auditors cannot exercise proper professional skepticism, which is a pillar of audit, without having the knowledge on what AI conclusions are based on quality.

Table 4: Key Themes from Auditor Interviews on AI Tool Transparency (N=25)

Theme	Frequency	Representative Quote
Trust Calibration Difficulty	84% (21/25)	"I don't know when to trust it and when to be skeptical because I can't see its reasoning"
Output Challenges (Validation)	76% (19/25)	"How do I verify a model's conclusion without essentially re-doing the entire analysis manually?"
Professional Concerns (Liability)	68% (17/25)	"At the end of the day, my name goes on the audit report. What happens when the AI misses something?"
Training Inadequacy	64% (16/25)	"We got a two-hour demo. That's not enough to really understand what the tool can and can't do"
Documentation Gaps	60% (15/25)	"The user manual tells you which buttons to click but not how to interpret what the model is telling you"

Validation challenges, reported by 76% of auditors, reflected the practical difficulty of independently verifying AI outputs without undermining automation efficiency. Auditors therefore faced a dilemma between accepting outputs with limited scrutiny or manually re-performing analyses. Both validation difficulty and obscurity overlap with professional liability issues. In case an AI tool does not identify a material misstatement, auditors are scared of having legal liabilities of failure to stop what they had no tools to stop. One partner said: The regulatory framework and legal precedents presuppose human decisions during the process of audit. Under delegation to AI, I am still the one holding the responsibility, but this time, there is no capacity to check the work as I could with human employees.

Developer and vendor views, although taking into account user concerns, are focused on constraints and trade-offs, which are invisible to end users. A recurring theme involved tension between transparency requirements and intellectual property protection. One product manager said: We can reveal all our model architecture and training strategy and have a copy within six months. We must have a degree of transparency in order to have competitive advantage. Developers further emphasized the technical limitations of explainability methods for complex ensemble and deep learning systems. with millions of parameters. Some of the participants claimed that the requirements of total transparency are unrealistic because of the complexity of the state of modern AI. They opined that it may be more feasible to concentrate on validation of outputs, as opposed to the comprehension of internals.

Regulatory participants highlighted institutional capacity limitations. The majority of them admitted to not having the technical means to test AI audit tools in-house and had to rely on the assurances of the vendors or third parties whose reliability was apparently questionable. According to one of the regulators: We have the ability to look through the traditional audit workpapers since we have knowledge on audit methodology. When using AI, we tend to see a black box and hope that it works as it promises to do. This asymmetry potentially weakens effective oversight by placing informational advantage in the hands of vendors and audit firms. instead of regulators. The representatives of audited entities were less concerned about

transparency technologically but outcome transparency and error accountability. Some of the respondents stated that they would not be opposed to opaque AI systems provided that they remain subject to transparent accountability measures, such that they would not be wrongly punished due to false positives or errors of the algorithm.

3.4 Gap Analysis and Comparative Performance

Fig. 4 demonstrates that the largest transparency gaps were associated with training data disclosure and model architecture transparency. A radar chart is provided in Figure 4, where the desired transparency level among the stakeholders is contrasted with the observed implementation in 6 key dimensions.

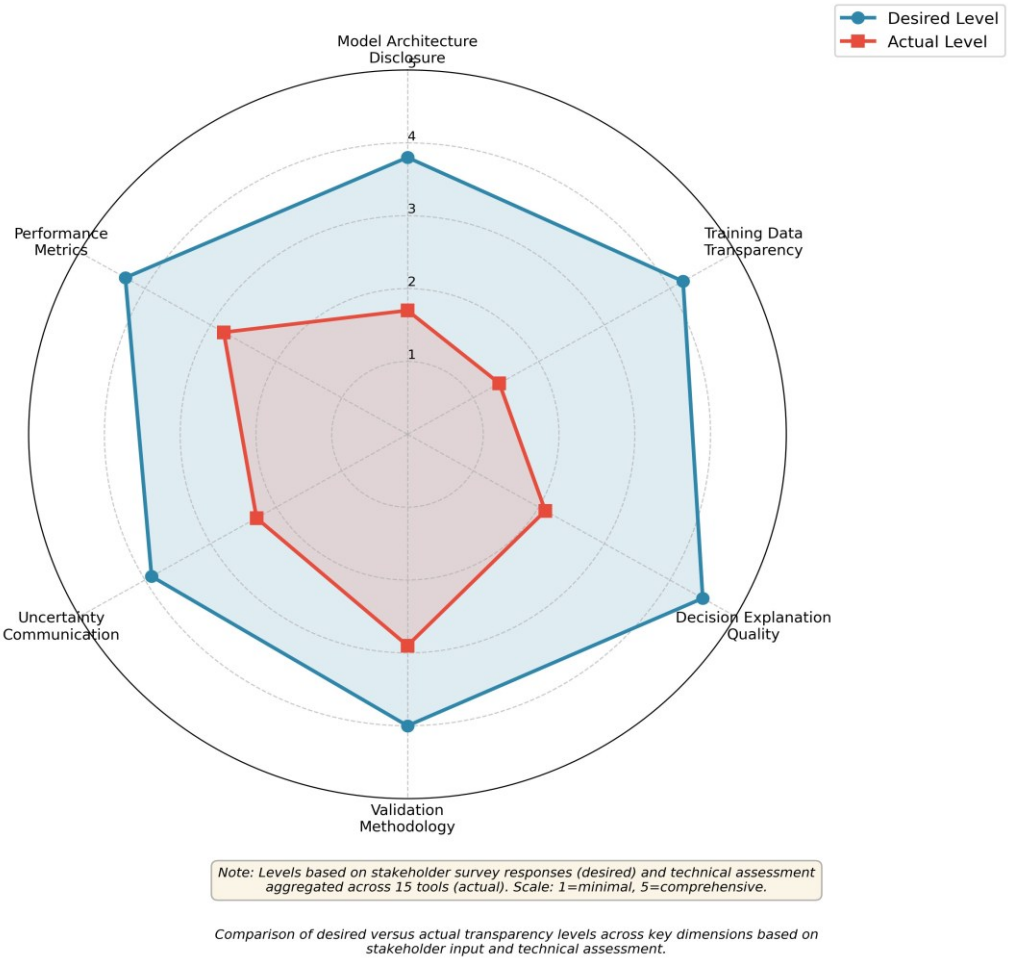


Fig. 4: Comparative analysis between desired and actual levels of transparency in the major dimensions in line with stakeholder input and technical evaluation.

Fig. 4 indicates that training data transparency (2.8-point gap), and model architecture disclosure (2.1-point gap) have the biggest gaps, which are exactly where the vendors reference competitive issues. Table 5 shows consistent results in the implementation of transparency and accountability between categories of tools. Table 5 indicates that there are no tool categories which perform well on all dimensions and therefore, there are trade-offs in them. Commercial vendors invested heavily in user interface quality and documentation while limiting disclosure of algorithmic details. The open-source projects offer transparency at the code level, but do not have a lot of resources to support large-scale documentation or audit trail.Table

Table 5: Comparative Performance Across Tool Categories

Dimension	Commercial (n = 8)	Open-Source (n = 3)	Proprietary (n = 4)	Overall Mean (N = 15)
Technical Transparency	2.1 / 5.0	3.8 / 5.0	2.3 / 5.0	2.4 / 5.0
Procedural Transparency	3.2 / 5.0	2.1 / 5.0	2.8 / 5.0	2.9 / 5.0
Audit Trail Features	2.9 / 5.0	1.9 / 5.0	3.1 / 5.0	2.7 / 5.0
User Interface Quality	3.8 / 5.0	2.2 / 5.0	3.3 / 5.0	3.3 / 5.0
Documentation Quality	3.6 / 5.0	2.5 / 5.0	2.9 / 5.0	3.1 / 5.0

3.5 Discussion of Findings

The findings have important implications for research, professional practice, and regulatory policy. To begin with, the transparency paradox is a reality that is subtle in nature. Increased transparency is always in demand among the stakeholders, but technical transparency is not enough to establish the right trust. The effectiveness of transparency depends not merely on the quantity of disclosed information but on its relevance, usability, and interpretability. A very technical description can render understanding of it impossible for the non-expert auditors and be of little practical use, though technically transparent. In its turn, the simplified and yet suitably focused explanation of the association between AI recommendations and the accepted audit notions can be helpful in decision-making without full disclosures of the algorithm. This implies that to have good transparency, there must be multiple layers of approaches that give varied information at varied levels of detail to users with different levels of expertise.

Some systems attempted to address this challenge through progressive disclosure interfaces, although implementation remained limited. Second, the findings suggest partial operational decoupling between transparency and accountability. A range of tools showed high procedural accountability, namely, a clear policy on governance with defined roles and responsibilities, an extensive audit trail over the use of the systems, strong validation procedures to evaluate system performance prior to its deployment, continuous monitoring to detect degradation, although with little algorithmic transparency about model internals. This defies the expectation that accountability is mandatory and therefore entails transparency. Although transparency can support accountability, accountability can be implemented in organizations using procedural measures that do not require full knowledge of the internals of the algorithms. This pattern was particularly evident in financial services environments where strong procedural controls compensated for limited algorithmic transparency. But the decoupling has its own limits manifested in the cases of failures. Procedural accountability in the absence of transparency may serve well in normal operations, but not in the case of system failure in unforeseen circumstances. Root cause analysis and corrective action are problematic without understanding why a model is behaving erratically. Can it be because distributional changes are afoot, or are there interactions between features and/or due to gaps in validation? Accountability mechanisms have no information that they can use to identify what, who, and how things went awry without minimum transparency that would help get the diagnosis of the failure mode. It implies that transparency and accountability can be operationally uncoupled, but some minimum transparency is required to achieve accountability in the long term, especially in the face of failures (Onwuegbuchi *et al*., 2023; Adeyemi, 2023).

Third, the patterns of trust and adoption are more complicated and multifaceted than anticipated. In contrast to the expectations that transparency will be a direct influence on

trust, we did not find a strong correlation between transparency characteristics measured and either user-reported trust or adoption rates. Tools that had elaborate explainability characteristics did not automatically gain more trust or wider adoption than those that had little transparency but other appealing characteristics. Other influences seemed equally effective: perceived accuracy of the validation results, organization support via the leadership support, peer use that leads to social proof, quality of training that influences the user competence, integration with the workflow, and vendor reputation. This fact means that the transparency might not be improved enough to promote adoption and reasonable trust. Rather, multidimensional solutions that can be implemented at once can be required: technical enhancements of explainability, organizational investment in organizational structures, professional growth through training, and cultural transformation to establish the right skepticism (Areghan, 2023). Finally, the relationship between transparency mechanisms and measurable improvements in audit quality remains empirically inconclusive, highlighting the need for further longitudinal and performance-based research. Finally, the relationship between transparency mechanisms and measurable improvements in audit quality remains empirically inconclusive, highlighting the need for further longitudinal and performance-based research.

4.0 Conclusion

This study provided an empirical evaluation of transparency and accountability mechanisms in AI-driven audit tools, revealing substantial heterogeneity and significant gaps between current implementations and stakeholder expectations. Although explainable AI and audit trail technologies demonstrate considerable technical potential, their implementation across commercial audit systems remains inconsistent and, in some cases, inadequate. The findings challenge simplistic assumptions that AI systems are either inherently trustworthy technological improvements or inevitably opaque and uninterpretable. Instead, the study highlights the complex trade-offs among transparency, competitive advantage, technical feasibility, and user requirements.

Based on these findings, this study proposed a multidimensional evaluation framework comprising technical transparency elements such as model interpretability and decision explanation, procedural accountability mechanisms including audit trails and governance controls, and organizational dimensions such as training programs and oversight structures. This framework may assist practitioners in evaluating AI audit tools, support vendors in prioritizing development strategies, and guide regulators in establishing appropriate compliance requirements.

However, meaningful transparency and accountability cannot be achieved through technical solutions alone. They also require organizational commitment, professional standard-setting, and effective regulatory oversight. The study was limited by sample size and restricted access to proprietary technical information from some vendors, which may have constrained the depth of comparative evaluation. Future research should explore the relationship between transparency mechanisms and measurable audit quality outcomes using longitudinal and industry-specific evidence.

As AI assumes an increasingly central role in audit practice, robust transparency and accountability mechanisms are essential not only for technical reliability but also for maintaining the profession's social legitimacy and public trust in financial reporting systems.

5.0 References

Aboagye, E. F., Borketey, B., Danquah, K., & Borketey, D. (2022). A predictive modeling approach for optimal prediction of the probability of credit card default. *International Research Journal of Modernization in*

Engineering Technology and Science, 4, 8, pp. 2425–2441.

(2) Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on explainable artificial intelligence (XAI). *IEEE Access*, 6, pp. 52138–52160. https://doi.org/10.1109/ACCESS.2018.2870052

Adeyemi, D. S. (2023). Autonomous response systems in cybersecurity: A systematic review of AI-driven automation tools. *Communication in Physical Sciences*, 9, 4, pp. 878–898.

Amoore, L., & Raley, R. (2017). Securing with algorithms: Knowledge, decision, sovereignty. *Security Dialogue*, 48, 1, pp. 3–10. https://doi.org/10.1177/0967010616680753

Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society*, 20, 3, pp. 973–989. https://doi.org/10.1177/1461444816676645

Areghan, E. (2023). From data breaches to deepfakes: A comprehensive review of evolving cyber threats and online risk management. *Communication in Physical Sciences*, 9, 4, pp. 738–753.

(Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. *European Law Journal*, 13, 4, pp. 447–468. https://doi.org/10.1111/j.1468-0386.2007.00378.x

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3, 2, pp. 77–101. https://doi.org/10.1191/1478088706qp063oa

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, pp. 451–468. https://doi.org/10.2308/acch-51023

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, 3, 1, pp. 1–12. https://doi.org/10.1177/2053951715622512

Coglianese, C., & Lehr, D. (2017). Regulating by robot: Administrative decision making in the machine-learning era. *Georgetown Law Journal*, 105, 5, pp. 1147–1223.

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). SAGE Publications.

DeFond, M., & Zhang, J. (2014). A review of archival auditing research. *Journal of Accounting and Economics*, 58, 2–3, pp. 275–326. https://doi.org/10.1016/j.jacceco.2014.09.002

Diakopoulos, N. (2016). Accountability in algorithmic decision making. *Communications of the ACM*, 59, 2, pp. 56–62. https://doi.org/10.1145/2844110

Dwork, C., Hardt, M., Pitassi, T., Reingold, O., & Zemel, R. (2012). Fairness through awareness. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, pp. 214–226. https://doi.org/10.1145/2090236.2090255

Dwork, C., & Mulligan, D. K. (2013). It's not privacy, and it's not fair. *Stanford Law Review Online*, 66, pp. 35–40.

(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, pp. 1–20. ht//doi.org/10.2308/jeta-10511

Kemper, J., & Kolkman, D. (2019). Transparent to whom? No algorithmic accountability without a critical audience. *Information, Communication & Society*, 22, 14, pp. 2081–2096. https://doi.org/10.1080/1369118X.2018.1477967

Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. *Journal of Emerging Technologies in*

Accounting, 14, 1, pp. 115–122. https://doi.org/10.2308/jeta-51730

Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. *University of Pennsylvania Law Review*, 165, 3, pp. 633–705.Lipton, Z. C. (2018). The mythos of model interpretability. *Queue*, 16, 3, pp. 31–57. https://doi.org/10.1145/3236386.3241340

Lundberg, S. M., & Lee, S. I. (2017). A unified approach to interpreting model predictions. In *Advances in Neural Information Processing Systems*, pp. 4765–4774.

Munoko, I., Brown-Liburd, H. L., & Vasarhelyi, M. (2020). The ethical implications of using artificial intelligence in auditing. *Journal of Business Ethics*, 167, 2, pp. 209–234. https://doi.org/10.1007/s10551-019-04407-1

Okolo, J. N. (2023). A review of machine and deep learning approaches for enhancing cybersecurity and privacy in the Internet of devices. *Communication in Physical Sciences*, 9, 4, pp. 754–772.

Onwuegbuchi, O., Ibiyeye, A. O., Okolo, J. N., & Adeniji, S. A. (2023). Cybersecurity risks in the fintech ecosystem: Regulatory and technological perspectives. *Communication in Physical Sciences*, 9, 4, pp. 947–967.

Passi, S., & Barocas, S. (2019). Problem formulation and fairness. In *Proceedings of the Conference on Fairness, Accountability, and Transparency*, pp. 39–48. https://doi.org/10.1145/3287560.3287567

Power, M. (1997). *The audit society: Rituals of verification*. Oxford University Press.

Ranerup, A., & Zinner Henriksen, H. (2019). Value positions viewed through the lens of automated decision-making: The case of social services. *Government Information Quarterly*, 36, 4, Article 101377. https://doi.org/10.1016/j.giq.2019.05.004\Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?" Explaining the predictions of any classifier. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 1135–1144. https://doi.org/10.1145/2939672.2939778

Selbst, A. D., & Barocas, S. (2018). The intuitive appeal of explainable machines. *Fordham Law Review*, 87, 3, pp. 1085–1139.

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review*, 20, 3, pp. 571–610. https://doi.org/10.5465/amr.1995.9508080331

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.

Declaration

Consent for publication

Not Applicable

Availability of data

Data shall be made available upon request

Ethical Considerations

Not applicable

Competing interest

The authors report no conflict or competing interest

Funding

The authors declared no source of funding

Authors' Contributions

Olatunde Ayeomoni conceptualized the study, supervised the research design, and coordinated the manuscript preparation. Sugar Raymond conducted data collection, technical analysis, and literature review. Jude Okwuchukwu Ogene contributed to case study evaluation, interpretation of findings, and manuscript editing. All authors reviewed and approved the final version of the manuscript.