ISSN: 2658-8455
Volume 7, Issue 13 (2026), pp. 678-701.
© Authors: CC BY-NC-ND

Internal Audit and Artificial Intelligence: A Narrative Review of Governance Conditions for Audit Effectiveness

Audit interne et intelligence artificielle : revue narrative des conditions de gouvernance de l'efficacité de l'audit

Imane BOUJMAL, ***(Doctorante)***
Ecole Nationale de Commerce et de Gestion Kénitra
Université Ibn Tofail de Kénitra, Maroc

Lotfi BENAZZOU, ***(Professeur de l'Enseignement Supérieur)***
Ecole Nationale de Commerce et de Gestion Kénitra
Université Ibn Tofail de Kénitra, Maroc

Adresse de correspondance :	ENCG Kenitra Ibn Tofaïl University, B.P 242 Kénitra, Maroc contact@uit.ac.ma (+212) 5 37 32 92 00
Déclaration de divulgation :	Les auteurs n'ont pas connaissance de quelconque financement qui pourrait affecter l'objectivité de cette étude. Ils assument l'entière responsabilité de tout éventuel plagiat, de l'usage de l'intelligence artificielle dans la rédaction, ainsi que des résultats présentés dans cet article.
Conflit d'intérêts :	Les auteurs ne signalent aucun conflit d'intérêts.
Citer cet article	BOUJMAL, I., & BENAZZOU, L. (2026). Internal Audit and Artificial Intelligence: A Narrative Review of Governance Conditions for Audit Effectiveness. *International Journal of Accounting, Finance, Auditing, Management and Economics*, *7*(13), 678–701. https://doi.org/10.5281/zenodo.23839071
Licence	**Cet article est publié en open Access sous licence CC BY-NC-ND**

Received: 24/09/2026 *Accepted: 30/10/2026*

Internal Audit and Artificial Intelligence: A Narrative Review of Governance Conditions for Audit Effectiveness

Abstract:

Artificial intelligence (AI) is reshaping organizational governance and, within it, the internal audit function. Research on AI in auditing has focused largely on external audit, on specific technologies or on ethical principles, and few contributions connect the theoretical foundations of governance and internal audit with the governance challenges that AI introduces. This paper therefore asks how AI is transforming internal audit and which governance conditions are required for this transformation to strengthen, rather than undermine, audit effectiveness, understood as analytical coverage, detection capacity, independence and quality of reporting. Based on a narrative and integrative review of 66 sources published between 1932 and 2026, and drawing on agency, contingency, neo-institutional, stakeholder and sociomaterial perspectives, the paper distinguishes data analytics, automation and AI in the strict sense, weighs the benefits of AI against its costs and limits, and develops a conceptual framework linking AI capabilities, AI governance mechanisms, the auditor's role and audit effectiveness, from which five theoretical propositions are derived. The review suggests that AI may enhance audit efficiency, broaden analytical coverage and strengthen fraud and anomaly detection, while simultaneously introducing governance risks related to algorithmic opacity, data quality, automation bias, accountability and auditor independence. The paper contributes by treating AI both as an audit tool and as an audit object, and by differentiating the managerial and regulatory implications for internal audit leaders, audit committees, senior management and regulators. It outlines precise research questions, hypotheses and designs for future empirical work, particularly in resource-constrained and public-sector contexts such as Moroccan public establishments.

Keywords: Artificial Intelligence, Internal Audit, AI Governance, Digital Transformation, Audit Effectiveness.
Classification JEL : M42, M15, O33.
Paper type: Narrative literature review with a conceptual aim.

Résumé :

L'intelligence artificielle (IA) transforme la gouvernance organisationnelle et, avec elle, la fonction d'audit interne. La recherche sur l'IA en audit s'est surtout concentrée sur l'audit externe, sur des technologies prises isolément ou sur des principes éthiques, et peu de travaux relient les fondements théoriques de la gouvernance et de l'audit interne aux défis de gouvernance que l'IA introduit. Cet article interroge donc la manière dont l'IA transforme l'audit interne et les conditions de gouvernance requises pour que cette transformation renforce, plutôt que fragilise, l'efficacité de l'audit, entendue comme la couverture analytique, la capacité de détection, l'indépendance et la qualité des rapports. Fondé sur une revue narrative et intégrative de 66 sources publiées entre 1932 et 2026, et mobilisant les perspectives de l'agence, de la contingence, néo-institutionnelle, des parties prenantes et de la sociomatérialité, l'article distingue l'analyse de données, l'automatisation et l'IA au sens strict, met en balance les bénéfices de l'IA et ses coûts et limites, et construit un cadre conceptuel reliant les capacités de l'IA, les mécanismes de gouvernance de l'IA, le rôle de l'auditeur et l'efficacité de l'audit, dont sont dérivées cinq propositions théoriques. La revue suggère que l'IA pourrait améliorer l'efficacité de l'audit, élargir la couverture analytique et renforcer la détection des fraudes et des anomalies, tout en introduisant des risques de gouvernance liés à l'opacité algorithmique, à la qualité des données, au biais d'automatisation, à la responsabilité et à l'indépendance de l'auditeur. L'article contribue en traitant l'IA à la fois comme outil et comme objet d'audit, et en différenciant les implications pour les responsables de l'audit interne, les comités d'audit, la direction générale et les régulateurs. Il formule des questions et des dispositifs de recherche précis pour de futurs travaux empiriques, en particulier dans les contextes contraints en ressources et dans le secteur public, tels que les établissements publics marocains.

Mots-clés: Intelligence artificielle, Audit interne, Gouvernance de l'IA, Transformation digitale, Efficacité de l'audit.
JEL Classification: M42, M15, O33.
Type du papier: Revue de littérature narrative à visée conceptuelle

ISSN: 2658-8455
Volume 7, Issue 13 (2026), pp. 678-701.
© Authors: CC BY-NC-ND
IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

1. Introduction

Organizations across sectors are undergoing a profound digital transformation that is redefining how value is created, risks are managed, and decisions are made (Bhimani & Willcocks, 2014). Among the technologies driving this shift, artificial intelligence (AI) occupies a distinctive place, unlike earlier waves of digitalization that primarily automated data processing, AI systems increasingly perform tasks that involve pattern recognition, prediction, and, in their most advanced forms, autonomous decision-making (Davenport & Ronanki, 2018; Raisch & Krakowski, 2021). This capacity to learn from data and act on it is not confined to any single business function; it cuts across finance, operations, marketing, and governance, prompting scholars to describe AI as a general purpose technology capable of transforming entire organizational architectures rather than isolated tasks (Bresnahan & Trajtenberg, 1995; Brynjolfsson et al., 2019).

Internal audit occupies a paradoxical position within this transformation. On one hand, as the function responsible for providing independent assurance over governance, risk management, and control processes (Institute of Internal Auditors [IIA], 2024), internal audit is directly affected by the same volume, velocity, and complexity of data that AI is designed to handle. On the other hand, internal audit has historically relied largely on retrospective, sample-based methodologies designed for a much slower and more limited information environment (Vasarhelyi et al., 2015), even though risk-based planning, computer-assisted audit techniques and continuous auditing had already extended its analytical reach before the advent of AI (Rezaee et al., 2002). The question is no longer hypothetical. In a global survey of internal audit leaders conducted in May 2024 (924 responses), about 62% of the functions answering the relevant question reported using generative AI in their activities or researching its future use, whereas only about 12.4% reported auditing generative AI within their organization (Internal Audit Foundation & Wolters Kluwer TeamMate, 2024). The survey is not representative of the whole profession, but it indicates the direction of practice.

This tension is compounded by a second, more subtle transformation : internal auditors are no longer only auditing organizations that use AI in their core operations. AI is also becoming part of the audit process itself. Internal auditors are increasingly expected to leverage AI tools such as machine learning, natural language processing, and robotic process automation to conduct their own work, while simultaneously developing the competencies needed to assess and provide assurance over the AI systems embedded in the organizations they audit (Anica-Popa et al., 2026). This dual role, AI as an audit tool and AI as an audit object, has received growing but still fragmented attention in the academic literature (Anica-Popa et al., 2026; Raji et al., 2020), and it raises governance questions that extend well beyond technical implementation, touching on auditor independence, algorithmic accountability, and the ethical use of automated systems in assurance work (Munoko et al., 2020).

The body of research on AI in accounting and auditing is growing. Influential contributions have set out research agendas for AI in auditing (Issa et al., 2016), described how automation is changing audit work (Kokina & Davenport, 2017), documented how AI investment in audit firms relates to audit quality and staffing (Fedyk et al., 2022) and examined the ethical challenges of AI-based decision-making in accounting and auditing (Lehner et al., 2022). Yet most existing studies either focus narrowly on external/financial audit (Appelbaum et al., 2017) or on specific technologies in isolation, without situating AI adoption within a broader conceptual framework of organizational governance (Anica-Popa et al., 2026). Few contributions explicitly connect the theoretical foundations of governance and internal audit as a regulatory mechanism with the practical and ethical challenges introduced by AI. This paper addresses that gap by placing internal audit, rather than the audit firm or the financial statements audit, at the center of the analysis.

The gap is particularly visible in public-sector and emerging-economy settings, where internal audit operates under budgetary rules, hierarchical control structures and uneven digital infrastructure, and where local research has addressed the digitalization of internal audit more than AI proper (Ait Lemqeddem & Chouay, 2020; El Haiba & Maimoun, 2024). Moroccan public establishments serve here as an illustrative context, which allows the paper to examine how far its arguments hold in settings where resources and regulation are constrained.

Against this background, the present paper addresses the following central question: how is artificial intelligence transforming the internal audit function, and what governance conditions are required for this transformation to enhance, rather than undermine, audit effectiveness? Audit effectiveness is understood here through four working criteria, consistent with the internal audit effectiveness literature (Gramling et al., 2004; Lenz & Hahn, 2015): analytical coverage, detection capacity, independence and objectivity, and quality of reporting. To answer the central question, it is broken down into three sub-questions (SQ1 to SQ3), each linked to one objective:

- SQ1: which conceptual foundations link organizational governance, internal audit and AI governance, and which theories explain their relationships? To clarify the conceptual foundations linking organizational governance, internal audit, and AI governance;
- SQ2: how are internal audit practices adapting to an AI-driven business environment, with AI as an audit tool and as an audit object, and with what benefits and risks? To analyze how internal audit practices are adapting to this environment, including the limitations of traditional methods and the technologies reshaping the profession;
- SQ3: which governance, organizational and contextual conditions determine whether this transformation strengthens audit effectiveness? To synthesize the findings in a conceptual framework and to discuss the managerial and theoretical implications of this transformation, together with avenues for future research.

The paper makes three contributions that go beyond a descriptive synthesis. First, it places internal audit at the center of the analysis and positions the review explicitly against earlier research agendas, empirical studies and ethical analyses (Fedyk et al., 2022; Issa et al., 2016; Kokina & Davenport, 2017; Lehner et al., 2022). Second, it treats AI both as an audit tool and as an audit object, which allows the review to address the benefits of AI-assisted audit and, at the same time, the assurance that internal audit must provide over the AI systems of the organization. Third, it integrates the findings in a conceptual framework and five theoretical propositions, and it differentiates the managerial implications by actor, namely internal audit leaders, audit committees, senior management and regulators.

Methodologically, the paper adopts a narrative and integrative literature review approach, consistent with the theoretical and exploratory nature of the research question. The remainder of the paper is structured as follows. Section 2 presents the research methodology and documents the review protocol. Section 3 develops the literature review in three parts. Section 3.1 covers the conceptual foundations, namely organizational governance, internal audit as a regulatory device and the emerging risks associated with AI governance. Section 3.2 examines how internal audit is adapting to an AI-driven environment, discussing the limitations of traditional audit methods, AI as an audit tool and as an audit object, the redefinition of the auditor's role through human-AI collaboration and the public-sector and Moroccan context. Section 3.3 presents an integrative conceptual framework and the five theoretical propositions derived from the review. Section 4 presents the results as a cross-cutting synthesis of the technologies, governance risks and tensions identified. Section 5 discusses the theoretical and managerial implications, the regulatory environment and the counter-arguments, and Section 6 concludes with the study's limitations and directions for future research.

ISSN: 2658-8455
Volume 7, Issue 13 (2026), pp. 678-701.
© Authors: CC BY-NC-ND
IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

2. Research Methodology

2.1 Review Design and Protocol

This study adopts a narrative and integrative literature review methodology, a design well suited to research questions that are conceptual and exploratory in nature, and that aim to synthesize a heterogeneous and rapidly evolving body of knowledge rather than test statistically formulated hypotheses (Snyder, 2019). Unlike systematic reviews, which typically apply rigid, preregistered search protocols to maximize replicability, narrative and integrative reviews prioritize the conceptual integration of insights across theoretical traditions and empirical contexts, which is appropriate given the paper's objective of connecting organizational governance theory, internal audit scholarship, and the emerging literature on AI governance (Snyder, 2019). In the typology of Paré et al. (2015), the review is closest to the narrative type, with a theory-development ambition. Its integrative logic follows Torraco (2005), who presents the integrative review as a way of generating new frameworks and perspectives from existing literature, and Webster and Watson (2002), who recommend a concept-centered rather than author-centered synthesis. To make the process traceable even though the review is not systematic, the protocol is organized along the four stages of the SALSA framework (Search, AppraisaL, Synthesis, Analysis), which Grant and Booth (2009) use to characterize review types.

2.2 Search Strategy and Corpus Constitution

Search. Two corpora were constituted. The foundational corpus gathers the theoretical and conceptual works on governance, accountability, organizational regulation, technology acceptance and general-purpose technologies on which the paper's conceptual framework relies, together with earlier work on continuous auditing; it is not bounded by date, because these works are cited for their conceptual contribution and not for their currency. The AI and audit corpus gathers empirical, conceptual and professional works on AI, analytics and automation in auditing, on AI governance and on the public-sector context; it covers 2015 to 2026, the period in which big data, machine learning and, more recently, generative and agentic AI entered audit research and practice. Table 1 summarizes the search protocol.

Table 1: Search protocol of the review

Element	Description
Databases and platforms	Google Scholar; Scopus; publisher platforms (American Accounting Association, Emerald, Elsevier, Springer, ACM)
Block A (technology)	"artificial intelligence" OR "machine learning" OR "robotic process automation" OR "natural language processing" OR "generative AI" OR "agentic" OR "algorithmic"
Block B (audit)	"internal audit" OR "internal auditor" OR "audit" OR "assurance" OR "continuous auditing"
Block C (governance)	"governance" OR "accountability" OR "independence" OR "risk" OR "audit effectiveness" OR "auditability"
Search string and fields	A AND B AND C, applied to titles, abstracts and keywords; French equivalents (« intelligence artificielle », « audit interne », « gouvernance ») for French-language and Moroccan sources
Foundational corpus	Targeted search by concept and author (agency, accountability, contingency, institutional theory, technology acceptance, general-purpose technologies, organizational regulation); no date limit
Period of the AI and audit corpus	2015 to 2026
Languages	English and French
Last update of the corpus	October 2026

Source : Authors.

Searches were run in Google Scholar and Scopus and were complemented by direct consultation of the publisher platforms of the most represented journals and by backward and forward citation tracking from a small set of seed articles identified at the outset, notably Anica-Popa et al. (2026) and Ouhoud and El Ouafa (2025). As the search was iterative and conceptual, the records screened at each step were not counted, so no flow diagram is reported; Table 3 instead presents the composition of the final corpus. Claims known only through another author's citation were traced to the original source or excluded.

2.3 Inclusion and Exclusion Criteria

Table 2 states the criteria applied to each corpus. Studies on external audit are retained only as comparators and are identified as such in the text. Textbooks are cited only for definitions, never to support claims about internal audit or about the economic characteristics of AI.

Table 2 : Inclusion and exclusion criteria by corpus

Criterion	Foundational corpus	AI and audit corpus
Document types	Seminal books and chapters; peer-reviewed articles	Peer-reviewed articles and conference papers; standards, regulations and institutional reports; scholarly chapters
Subject	Governance, accountability, organizational regulation, organizational and technology theory, continuous auditing	AI, analytics or automation in internal or external audit; AI governance and algorithmic auditing; public-sector and Moroccan context
Period	No limit	2015 to 2026
Languages	English, French	English, French
Exclusion	Works without conceptual contribution to the argument; textbooks used to support substantive claims	Vendor marketing material, student theses and notes, undocumented press reports, works known only through secondary citation

Source: Authors.

2.4 Quality Appraisal and Corpus Composition

Appraisal. Sources were classified in three evidence levels, which govern how each one is used. Level 1 comprises peer-reviewed journal articles and conference papers; they support substantive claims and any empirical figure, and, within this level, local-journal sources on the Moroccan context are used for context and flagged as such. Level 2 comprises standards, regulations and professional or institutional publications; they support statements about normative requirements and professional practice but not causal claims. Level 3 comprises scholarly books and chapters, used for theory and definitions. Quantitative claims (time savings, cycle-time reductions, sampling ratios) are reported only when the primary study is identified; otherwise they are flagged as secondary figures or omitted.

Table 3 : Composition of the final corpus by source type and corpus

Source type	Foundational corpus	Methodological corpus	AI and audit corpus	Total
Peer-reviewed journal articles and conference papers (level 1)	14	5	25	44
Standards, regulations and professional or institutional publications (level 2)	0	0	10	10
Scholarly books and chapters (level 3)	9	0	3	12
Total	***23***	***5***	***38***	***66***

Source: Authors' compilation from the final reference list.

Table 3 shows that the final corpus comprises 66 sources: 23 in the foundational corpus, 5 in the methodological corpus and 38 in the AI and audit corpus. The oldest source dates from 1932 and the most recent from 2026.

ISSN: 2658-8455
Volume 7, Issue 13 (2026), pp. 678-701.
© Authors: CC BY-NC-ND
IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

2.5 Synthesis Procedure and Reflexivity

Synthesis and analysis. Each source was coded in a concept matrix (Webster & Watson, 2002) along five constructs derived from the research question: AI capabilities, AI governance mechanisms, the auditor's role, risks, and audit effectiveness, with the context (public sector, regulation, resources) coded as a sixth variable. Themes were identified inductively and then grouped under these constructs; contradictions between sources were documented and not smoothed, which led to the tensions presented in Section 4. The matrix also served to compare the two roles of AI (tool and object) and to identify where the evidence is thin.
Reflexivity. The authors work on internal audit in Moroccan public establishments, which may orient source selection toward public-sector and resource-constrained contexts. To limit this risk, the selection criteria were made explicit (Table 2), counter-evidence on adoption limits, automation bias and deskilling was sought actively, and the context is treated in a dedicated subsection (Section 3.2.5). Coding was carried out by a single researcher; no second coder or expert panel validated the corpus, which is acknowledged as a limitation in Section 6.

3. Literature Review

3.1 Conceptual Foundations of Governance, Internal Audit and AI

3.1.1 Organizational Governance: Actors, Mechanisms and Purposes

Organizational governance can be defined as the set of formal and informal mechanisms that structure relationships among an organization's stakeholders in order to ensure value creation and long-term sustainability (Charreaux, 1997). It involves a plurality of actors (shareholders, boards of directors, executive management, employees and, more broadly, external stakeholders such as regulators and communities) whose interests do not always converge (Berle & Means, 1932). Governance mechanisms are conventionally divided into external mechanisms, such as capital markets, regulation, and external audit, and internal mechanisms, such as the board of directors, internal control systems, and internal audit (Charreaux, 1997).
These mechanisms serve several complementary purposes: aligning the interests of principals and agents, curbing opportunistic behavior, improving organizational performance, and reinforcing the legitimacy of the organization in the eyes of its stakeholders (Jensen & Meckling, 1976). Agency theory, in particular, has provided one of the most influential lenses for understanding governance: because managers (agents) may pursue objectives that diverge from those of owners (principals), organizations require monitoring devices capable of reducing information asymmetries and aligning incentives (Jensen & Meckling, 1976). Internal control and internal audit are commonly regarded as central instruments for operationalizing this monitoring function (Anthony & Govindarajan, 2007). The classical principal-agent lens has two limits for the present purpose. First, internal audit serves the board, the audit committee and executive management simultaneously, so the relationship it monitors involves multiple principals with potentially divergent expectations (Gramling et al., 2004). Second, agency theory says little about the sociotechnical character of AI. The paper therefore complements it with three perspectives: neo-institutional theory, which explains why organizations adopt practices partly to secure legitimacy under coercive, mimetic and normative pressures (DiMaggio & Powell, 1983); stakeholder theory, which widens the set of parties to whom assurance is owed (Freeman, 1984); and sociomateriality, which treats technology and organizing as mutually constitutive (Orlikowski & Scott, 2008).
A concept closely associated with governance is accountability, understood as the obligation of an actor to justify decisions, actions and the use of resources entrusted to them (Roberts & Scapens, 1985). Bovens (2007) conceptualizes accountability as a relationship between an actor and a forum, in which the actor must explain and justify conduct and the forum may question

it, pass judgment and impose consequences. Building on this relational view, the paper distinguishes three dimensions of accountability that structure the analysis: financial, managerial and informational. This distinction is particularly relevant because AI interacts with each dimension differently: it may improve the traceability of information while complicating the explainability of automated decisions (Pasquale, 2015).Contingency theory offers a complementary perspective, arguing that there is no single optimal organizational structure; rather, effectiveness depends on an organization's capacity to adapt its structures and control mechanisms to a changing environment (Donaldson, 2001). Applied to governance, this suggests that as organizational environments become more data-intensive, volatile, and technologically complex, governance mechanisms, including internal audit, must evolve accordingly rather than remain fixed in their traditional form (Donaldson, 2001). This adaptive view of governance sets the stage for understanding internal audit not as a static compliance function but as a mechanism that is itself subject to transformation.

3.1.2 Internal Audit as a Mechanism of Organizational Regulation

In organizational sociology, regulation designates the production and maintenance of the rules that orient collective action and reconcile autonomy with control (Reynaud, 1989), and audit has been analyzed as a ritual of verification that renders organizations visible and governable (Power, 1997). Internal audit can accordingly be understood as a mechanism of organizational regulation: a device that structures behavior, orients decisions, and maintains an equilibrium between operational autonomy and control, in line with the management control tradition (Anthony & Govindarajan, 2007). The Global Internal Audit Standards, published by the Institute of Internal Auditors in 2024 and effective since 9 January 2025 in replacement of the 2017 International Professional Practices Framework, state that internal auditing strengthens an organization's ability to create, protect, and sustain value by providing the board and management with independent, risk-based, and objective assurance, advice, insight, and foresight (IIA, 2024). This definition situates internal audit at the intersection of three organizational domains that recur throughout the literature: governance, risk management, and internal control (IIA, 2024; Anica-Popa et al., 2026).

Historically, internal audit emerged largely as an institutional response to major financial scandals of the twentieth century, evolving from a narrow focus on financial verification toward a broader mandate encompassing operational, strategic, and compliance risks (Anica-Popa et al., 2026). Unlike external or financial audit, which is typically performed by independent firms to provide statutory assurance to external stakeholders on the accuracy of financial statements, internal audit is carried out by employees or co-sourced professionals operating under the oversight of management and the audit committee, and its scope extends well beyond financial reporting to include the evaluation of governance structures and operational controls (Anica-Popa et al., 2026).

As a regulatory mechanism, internal audit performs its function through a recurring cycle of planning, evidence collection, analysis, and reporting, in which auditors typically rely on sampling techniques to draw conclusions about entire populations of transactions or processes (Chan & Vasarhelyi, 2011). This approach reflects a longstanding trade-off between the cost of exhaustive verification and the need for reasonable assurance. However, this trade-off is precisely what is being challenged by the growing volume, velocity, and variety of organizational data, a tension explored in greater depth in Section 3.2.1.

Internal audit's regulatory role is reinforced by professional frameworks such as the IIA's Global Internal Audit Standards (IIA, 2024) and, more broadly, by the COSO Internal Control: Integrated Framework, whose five components structure the assessment of internal control systems around the control environment, risk assessment, control activities, information and communication, and monitoring activities (Committee of Sponsoring Organizations of the

ISSN: 2658-8455
Volume 7, Issue 13 (2026), pp. 678-701.
© Authors: CC BY-NC-ND
IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

Treadway Commission [COSO], 2013). The 2013 framework already recognizes the growing importance of technology for internal control, notably through its principle on general control activities over technology (COSO, 2013), while the COSO Enterprise Risk Management framework addresses the distinct question of integrating risk management with strategy and performance (COSO, 2017). The 2024 Standards likewise require the chief audit executive to ensure that the function has the technological resources needed to support the audit process (IIA, 2024, Standard 10.3), which signals an institutional recognition that technological change increasingly shapes the terrain on which internal audit operates.

3.1.3 AI Governance and Emerging Risks in Organizations

AI governance can be defined as the set of principles, structures, and processes that organizations put in place to ensure that AI systems are developed and used in a manner that is transparent, accountable, and aligned with organizational and societal values (Munoko et al., 2020; Lehner et al., 2022). Unlike traditional information technologies, AI systems, particularly those based on machine learning and deep learning, derive their behavior from patterns learned from historical data rather than from explicitly programmed rules. This characteristic introduces a set of governance challenges that are qualitatively different from those associated with earlier generations of enterprise technology (Anica-Popa et al., 2026).

The first and most widely discussed challenge is algorithmic opacity, often described through the black box metaphor (Pasquale, 2015). Opacity may stem from proprietary secrecy, from the technical illiteracy of those who must assess a model, or from the mismatch between high-dimensional machine learning and human-scale reasoning (Burrell, 2016). When the internal logic of a model is not readily interpretable, auditors, managers and regulators struggle to understand how an output was produced, which complicates efforts to justify or challenge automated decisions (Casper et al., 2024). Opacity is compounded by algorithmic bias: because AI systems learn from historical data, they can reproduce or even amplify the biases it contains, leading to discriminatory or otherwise flawed outcomes (O'Neil, 2016). Data quality is a second major risk area, since incomplete, noisy or unrepresentative data can generate false positives, mask genuine anomalies or produce misleading analytical conclusions (Zhang et al., 2022).

A third concern is accountability dilution. As decision-making authority is partially delegated to automated systems, it becomes unclear who is responsible when an AI-supported decision proves wrong: the developer of the algorithm, the organization deploying it or the professional relying on its output (Raji et al., 2020; Lehner et al., 2022). This concern is particularly acute for internal auditors, whose professional value rests on independent judgment (Baldwin et al., 2006). If auditors defer uncritically to algorithmic outputs, a pattern documented in human-factors research as automation bias (Parasuraman & Manzey, 2010), their independence and the credibility of their assurance may be compromised. A study of external auditors in an emerging market points in the same direction (Kamareldawla, 2025).

Institutional and professional bodies have started to respond. The IIA's 2024 Standards embed technology considerations in the governance of the internal audit function (IIA, 2024). ISO/IEC 42001:2023 specifies requirements for an AI management system (International Organization for Standardization & International Electrotechnical Commission [ISO/IEC], 2023); the NIST AI Risk Management Framework 1.0 organizes AI risk management around the functions govern, map, measure and manage (Tabassi, 2023); and Regulation (EU) 2024/1689 introduces a risk-based legal regime for AI systems (European Union, 2024). Section 5.3 compares these instruments. However, several studies note that these guidelines remain largely principle-based and offer limited operational detail on how organizations, and internal audit functions in particular, should translate them into practice (Anica-Popa et al., 2026).

In sum, AI governance emerges as a necessary extension of organizational governance: it must address not only the traditional agency problem between principals and managers, but also the

added complexity of non-human, adaptive decision-making systems. This foundation sets the stage for Section 3.2, which examines how internal audit, as one of the organization's principal regulatory mechanisms, is adapting to this AI-driven environment.

3.2 Adapting Internal Audit to an AI-Driven Business Environment

3.2.1 Limitations of Traditional Internal Audit and Earlier Innovations

Traditional internal audit methods were designed for an organizational environment characterized by manageable data volumes and predominantly manual information processes. Historically, auditing methods have often relied heavily on repetitive manual tasks (document review, reconciliation and face-to-face verification) that are prone to human error and time-consuming to execute (Anica-Popa et al., 2026). This reliance on manual procedures inherently limits the scope and frequency of audit engagements, as auditors must ration their attention across a finite set of priorities within constrained timeframes (Chan & Vasarhelyi, 2011).

A major limitation, however, concerns the reliance on representative sampling. Because it is impractical to manually examine every transaction in a large organization, auditors traditionally select a subset of transactions for testing and extrapolate their conclusions to the broader population (Anica-Popa et al., 2026). Because such samples cover only part of the transaction population, anomalies falling outside the sampled subset can go undetected, sometimes until a later audit cycle (Anica-Popa et al., 2026). The coverage ratio varies considerably across organizations and engagement types. In a digitalized business environment where millions of transactions can occur within a single day, this sampling-based logic becomes increasingly disconnected from the actual risk profile of the organization (Vasarhelyi et al., 2015).

A related limitation concerns the fundamentally retrospective orientation of traditional internal audit. Because manual procedures depend on the availability of completed records and finalized transactions, internal audit has typically operated as an ex-post verification mechanism, identifying issues only after they have already affected organizational outcomes (Rezaee et al., 2002). This retrospective posture stands in tension with the expectations of contemporary boards, audit committees, and regulators, who increasingly demand faster, more proactive, and more predictive insights into organizational risk (Ouhoud & El Ouafa, 2025).

Traditional practice, however, has never been purely manual. Risk-based audit planning concentrates effort where exposure is highest; computer-assisted audit techniques have long allowed population-level tests of data; and continuous auditing and continuous monitoring were conceptualized well before the current wave of AI (Chan & Vasarhelyi, 2011; Rezaee et al., 2002). AI therefore extends, rather than creates, the move toward data-driven assurance. It is useful to distinguish three layers: data analytics (descriptive and rule-based tests on full populations), automation (software executing predefined rules, as in robotic process automation) and AI in the strict sense (systems that learn from data to classify, predict or generate) (Moffitt et al., 2018; Russell & Norvig, 2021; Vasarhelyi et al., 2015). These layers are often conflated in the literature, which can overstate the specific contribution of AI.

Finally, traditional methods struggle to accommodate the growing heterogeneity of organizational data. Beyond structured financial records, auditors are increasingly confronted with vast quantities of unstructured data (contracts, emails, chat logs, sensor data) that cannot be efficiently analyzed using conventional spreadsheet-based techniques (Anica-Popa et al., 2026). Taken together, these limitations (the reliance on manual and sample-based verification, the retrospective orientation, and the difficulty of processing unstructured data at scale) form part of the structural rationale for internal audit's ongoing transformation through artificial intelligence, discussed in Section 3.2.2.

ISSN: 2658-8455
Volume 7, Issue 13 (2026), pp. 678-701.
© Authors: CC BY-NC-ND
IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

3.2.2 Artificial Intelligence as an Audit Tool: Technologies and Capabilities

AI is understood here broadly, following the agent-based perspective of Russell and Norvig (2021), as systems that perceive an environment and act to achieve goals; machine learning is the subset in which behavior is learned from data rather than explicitly programmed. The integration of AI into internal audit can represent a shift away from sample-dependent, compliance-oriented audits toward more sophisticated, predictive, and increasingly continuous models of assurance (Anica-Popa et al., 2026). Rather than merely accelerating existing manual procedures, AI can enable a data-driven approach in which automated processes support faster, more comprehensive, and more pervasive evaluations of organizational health (Anica-Popa et al., 2026).

Several families of technology underpin this transformation. Machine learning (ML) techniques allow systems to learn from historical transactional data in order to identify patterns, predict risks, and flag deviations that would be difficult for a human reviewer to detect manually (Issa et al., 2016; Kokina & Davenport, 2017). Natural language processing (NLP) extends these capabilities to unstructured textual data, enabling the automated analysis of contracts, correspondence, and reports in search of inconsistencies or red flags (Kokina & Davenport, 2017; Ouhoud & El Ouafa, 2025). Robotic process automation (RPA) targets the automation of repetitive, rules-based tasks such as data extraction, cross-validation of invoices against purchase orders, and compliance threshold checks, freeing auditors to focus on higher-value analytical work (Davenport & Ronanki, 2018; Moffitt et al., 2018). Automation can also improve the consistency and completeness of routine controls (Moffitt et al., 2018).

More recent technological developments point toward an even deeper transformation. Retrieval-augmented generation (RAG) architectures couple large language models with external knowledge bases, allowing AI systems to ground their outputs in verifiable organizational documents (policies, regulatory texts, prior audit reports), thereby mitigating the risk of factually incorrect or fabricated outputs, commonly referred to as hallucinations (Anica-Popa et al., 2026). Complementing this, vector databases provide the underlying infrastructure for semantic search across large, heterogeneous repositories of structured and unstructured data, which is particularly valuable in audit environments characterized by vast and diverse organizational data lakes (Anica-Popa et al., 2026). At the frontier of this evolution, agentic AI systems move beyond passive prediction toward autonomous, goal-directed behavior: rather than simply responding to a single prompt, an agentic system can decompose a complex audit objective into sub-tasks, retrieve relevant data, and coordinate a sequence of actions with limited human intervention (Anica-Popa et al., 2026). The evidence base on these developments remains nascent and largely conceptual, and rests mainly on a single recent source (Anica-Popa et al., 2026), so these developments should be read with caution.

These technologies translate into concrete audit capabilities. Automation reduces the manual burden of repetitive procedures such as transaction testing, data reconciliation and documentation (Anica-Popa et al., 2026). Anomaly detection algorithms allow auditors to analyze entire populations of transactions rather than samples and to identify irregular patterns that may indicate fraud or operational failure (Zhang et al., 2022). Predictive analytics extends this capability by helping internal audit anticipate emerging risks and control weaknesses, thereby supporting continuous auditing, a model in which monitoring is embedded in operational systems rather than performed periodically (Chan & Vasarhelyi, 2011). Empirical evidence, although limited, points in the same direction: in audit firms, greater AI investment is associated with improved audit quality and with changes in staffing structure (Fedyk et al., 2022), although this evidence concerns external audit. These capabilities also come with costs and limits. Implementation requires data infrastructure, specialized skills and sustained investment; reliance on third-party providers creates dependence and exposes audit data to

cybersecurity and confidentiality risks, particularly when sensitive information is submitted to external generative models (Tabassi, 2023); the energy consumption of large models adds an environmental cost (Strubell et al., 2019); and audit evidence produced by systems that are probabilistic and sometimes opaque is harder to document and defend than evidence produced by deterministic procedures (Casper et al., 2024). The gains described above are therefore conditional, not automatic.

The literature also emphasizes that AI adoption in internal audit is not without risk. Without a coherent conceptual framework and clearly defined governance mechanisms, AI integration can generate algorithmic bias, over-reliance on automated outputs, and fragmented or inconsistent implementations across the organization (Anica-Popa et al., 2026). This observation reinforces the point made in Section 3.1.3: technological capability alone is insufficient; it must be embedded within a governance structure that preserves the reliability and independence of the audit function. It also motivates the next subsections, which examine AI as an object of audit (Section 3.2.3) and the redefinition of the relationship between human auditors and AI systems (Section 3.2.4).

3.2.3 Artificial Intelligence as an Audit Object: Auditing AI Systems

The audit of AI systems has received less attention than the use of AI as an audit tool, and the 2024 survey cited above suggests that few internal audit functions yet audit the generative AI used in their organization (Internal Audit Foundation & Wolters Kluwer TeamMate, 2024). Auditing AI systems means providing assurance on how models are inventoried, designed, trained, validated, deployed and monitored, and on the quality and lawfulness of the data they use.

Raji et al. (2020) propose an end-to-end framework for internal algorithmic auditing, organized in five stages (scoping, mapping, artifact collection, testing and reflection) and designed to be embedded along the development lifecycle, so that audit is no longer a purely ex post exercise. In an internal audit setting, this logic implies model inventories, documentation of intended use, test evidence and a reflection stage in which residual risks are explicitly accepted by accountable owners. Lehner et al. (2022) add a normative dimension by showing that AI-based decision-making in accounting and auditing raises ethical questions that technical validation alone cannot settle.

Auditability, however, has limits. Casper et al. (2024) argue that black-box access, that is, the ability to query a model without access to its internals, training data or documentation, is insufficient for rigorous audits and that deeper access is needed; Verma et al. (2025) examine the conditions under which AI can be auditable at all. For internal audit, this raises three practical difficulties: access to vendor models is often restricted by contract, auditors may lack the technical competence to test models, and objectivity may be threatened when the function advises on the design of AI controls and later provides assurance over them, a threat that the 2024 Standards require to be safeguarded (IIA, 2024, Domain II). Most items in the corpus treat AI as a tool rather than as an object, which is itself a finding (Section 4).

3.2.4 Human-AI Collaboration: Redefining the Auditor's Role

A recurring theme across the literature is that AI is intended to augment, rather than replace, the internal auditor (Anica-Popa et al., 2026; Ouhoud & El Ouafa, 2025). This copiloted model of auditing positions AI as an audit-focused assistant that surfaces insights, drafts preliminary analyses, and flags anomalies, while the auditor retains responsibility for managing the audit process, validating findings, and exercising professional judgment (Anica-Popa et al., 2026). Process knowledge (an understanding of how a business actually operates, beyond what is captured in the data) remains indispensable for interpreting the anomalies that AI systems surface and for drawing appropriate conclusions in the final audit report (Anica-Popa et al., 2026).

ISSN: 2658-8455
Volume 7, Issue 13 (2026), pp. 678-701.
© Authors: CC BY-NC-ND
IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

This redefinition of roles requires a substantial evolution in auditor competencies. Traditionally trained in financial analysis, auditing standards, and internal control techniques, internal auditors must now develop hybrid skill sets spanning data analytics, information technology, and a working understanding of how machine learning models function, including their risks and limitations (Kokina & Davenport, 2017; Ouhoud & El Ouafa, 2025). One study reports that the positive effect of AI on internal audit quality is more pronounced among auditors who possess an information-technology background (Ouhoud & El Ouafa, 2025), which, although not generalizable on its own, underscores the practical importance of this competency shift. According to the same source, several large professional services firms have responded by introducing internal certifications in digital auditing. Automation also carries a risk of complacency and automation bias (Parasuraman & Manzey, 2010) and, more speculatively, of skill degradation if routinized tasks no longer exercise the tacit skills on which professional judgment depends. Big data may also affect auditor judgment through information overload and confirmation bias (Brown-Liburd et al., 2015).

The adoption of AI by auditors is also shaped by behavioral and organizational factors beyond technical competence. Drawing on the Technology Acceptance Model, perceived usefulness and perceived ease of use are identified as key determinants of auditors' willingness to adopt AI tools in their daily practice (Davis, 1989). The Unified Theory of Acceptance and Use of Technology extends this view with performance expectancy, effort expectancy, social influence and facilitating conditions, whose effects are moderated by age, gender, experience and voluntariness of use (Venkatesh et al., 2003). Organizational variables often invoked in audit studies, such as corporate culture, managerial support and normative pressure, are not moderators in either model; they are better captured by social influence and facilitating conditions, or through neo-institutional arguments (DiMaggio & Powell, 1983). Research applying such models to auditors indicates that individual characteristics and contextual factors both shape technology implementation decisions in auditing (Curtis & Payne, 2008). Where auditors receive adequate training, user-friendly tools, and clear governance guidance, they are considerably more likely to integrate AI meaningfully into their practice; conversely, resistance is more likely where auditors fear being replaced, distrust algorithmic transparency, or perceive a loss of professional autonomy (Ouhoud & El Ouafa, 2025).

This evolving division of labor between humans and machines also has direct implications for auditor independence, a cornerstone of the profession. Some internal auditors describe artificial intelligence as a gatekeeper function, ensuring accountability for organizational information and safeguarding stakeholder interests in an increasingly data-driven environment, while insisting that the human element of judgment remains indispensable to this role (Anica-Popa et al., 2026). At the same time, the opacity of certain AI models raises the risk that auditors may come to rely uncritically on algorithmic outputs, particularly where those outputs are favorably received by management, thereby subtly eroding the auditor's intellectual independence (Ouhoud & El Ouafa, 2025). Research on human trust in AI indicates that trust is shaped by features such as transparency and reliability (Glikson & Woolley, 2020), so that calibrated reliance, neither blind nor dismissive, becomes central to the auditor's role. Concepts such as AI auditability (the capacity to verify that an intelligent system's outputs are traceable, explainable and subject to independent scrutiny) and calls for what has been termed adaptive algorithmic oversight reflect an emerging view in the literature that human supervision must remain an explicit and structured feature of AI-augmented audit engagements, rather than an informal afterthought (Ouhoud & El Ouafa, 2025; Verma et al., 2025).

Taken together, these developments suggest that the transformation of internal audit through AI is best understood not as a simple substitution of human labor by machines, but as a reconfiguration of the auditor's role toward oversight, interpretation, and governance of

increasingly autonomous systems, a shift that has direct implications for how internal audit functions should be structured, trained, and evaluated going forward.

3.2.5 Public-Sector Internal Audit and the Moroccan Context

These benefits, however, are neither automatic nor evenly distributed. Research conducted in the Moroccan context illustrates this unevenness, with an important caveat: the two local studies available address the digitalization of internal audit rather than AI as such. Studies of digitalization in public organizations suggest that the adoption of digital tools can improve internal audit efficiency, but only where accompanied by adequate organizational adaptation (Ait Lemqeddem & Chouay, 2020). Conversely, research on Moroccan public establishments highlights how structural constraints (the absence of standardized information systems, regional disparities and digital skills shortages) can limit the practical gains of digitalization (El Haiba & Maimoun, 2024); whether the same constraints would limit AI remains to be tested. Alami Gholami and Lotfi (2026) address AI and internal audit in the banking sector, a regulated setting that offers a useful point of comparison for public establishments.

The institutional frame of Moroccan public internal audit also matters. The 2011 Constitution entrusts the Cour des comptes with the supreme control of public finances (article 147) and subjects public services to norms of quality, transparency, accountability and responsibility (article 154), which defines the accountability setting of audit functions (Royaume du Maroc, 2011). Law 09-08 on the protection of personal data, supervised by the National Commission for the Control of Personal Data Protection (CNDP), constrains the use of AI tools that process personal data, for instance when audit files containing staff or beneficiary data are submitted to external models (Royaume du Maroc, 2009).

Features specific to public internal audit, such as budget and procurement rules, a strong compliance orientation, statutory reporting lines and the status of auditors, are likely to condition both the adoption of AI and the form taken by its governance. No empirical study identified in this review tests these conditions for AI in Moroccan public establishments; they are therefore formulated as a proposition (Section 3.3.2). A weak regulatory framework does not necessarily lower trust in algorithmic outputs. Evidence from the Jordanian profession documents perceptions of AI's impact on auditing (Pérez-Calderón et al., 2025), but weak oversight may equally favor uncontrolled adoption and over-reliance, which is why the framework treats regulatory strength as a moderator whose effect may be non-linear.

3.3 Integrative Conceptual Framework and Theoretical Propositions

3.3.1 Integrative Conceptual Framework

Figure 1 integrates the constructs identified in the review (Sections 3.1 and 3.2). It links four constructs: AI capabilities (AI as audit tool and as audit object), AI governance mechanisms, the auditor's role and human oversight, and audit effectiveness (coverage, detection, independence and quality of reporting), all within an institutional and organizational context. The framework articulates four theoretical lenses: agency theory (delegation, monitoring and information asymmetry), contingency theory (fit between governance and context), neo-institutional theory (legitimacy pressures that shape governance choices) and sociomateriality (the entanglement of tool and practice).

ISSN: 2658-8455
Volume 7, Issue 13 (2026), pp. 678-701.
© Authors: CC BY-NC-ND
IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

Figure 1: Integrative conceptual framework of AI, governance and internal audit effectiveness

AI capabilities As audit tool: analytics, RPA, machine learning, NLP and generative AI, agentic systems As audit object: models, data and controls to be assured	**P1** direct, uneven effect	**Auditor's role and human oversight** AI literacy Structured critical oversight Calibrated reliance (risk of automation bias)	**P3** mediation	**Audit effectiveness** Analytical coverage Detection capacity Independence and objectivity Quality of reporting
Assurance over AI systems (P4) Limited by opacity, access to models and competence	**P2** moderation	**AI governance mechanisms** Model inventory Validation and documentation Explainability requirements Allocation of accountability Access rights to models		
Institutional and organizational context (P5: moderates all relationships, possibly in a non-linear way) Regulatory framework; data infrastructure and resources; public-sector features (budget rules, compliance orientation, reporting lines)				

Source : Authors' elaboration.

The labels P1 to P5 in Figure 1 refer to the propositions stated in Section 3.3.2. In short, AI capabilities are expected to affect audit effectiveness directly but unevenly (P1); AI governance mechanisms moderate this effect (P2); the auditor's role mediates it (P3); the capacity to provide assurance over AI as an object depends on access and competence (P4); and the context moderates all relationships (P5).

3.3.2 Theoretical Propositions

Table 4: Theoretical propositions derived from the review

No.	Proposition	Theoretical anchor	Main supporting sources
P1	Greater use of AI as an audit tool is positively associated with analytical coverage and detection capacity, whereas its association with independence and quality of reporting is not automatic and depends on P2 and P3.	Agency theory (monitoring capacity)	Fedyk et al. (2022); Zhang et al. (2022); Kokina & Davenport (2017)
P2	AI governance mechanisms (model inventory, validation and documentation, explainability requirements, allocation of accountability) moderate the relationship between AI use and audit effectiveness: the stronger the mechanisms, the more the benefits materialize and the lower the risks.	Contingency theory; neo-institutional theory	Raji et al. (2020); Lehner et al. (2022); Tabassi (2023)
P3	The effect of AI on audit effectiveness is mediated by the auditor's role: structured critical oversight and AI literacy increase effectiveness, whereas automation bias and over-reliance erode independence and quality of reporting.	Sociomateriality; trust in AI	Parasuraman & Manzey (2010); Glikson & Woolley (2020); Ouhoud & El Ouafa (2025)
P4	The capacity of internal audit to provide assurance over AI systems is limited by model opacity, restricted access to vendor models and competence gaps, and increases with contractual access rights and specialized skills.	Agency theory (information asymmetry)	Casper et al. (2024); Raji et al. (2020); Verma et al. (2025)
P5	Organizational and institutional maturity (data infrastructure, resources, regulatory framework, public-sector features) moderates all the relationships above, and its effect may be non-linear: weak oversight can favor uncontrolled adoption and over-reliance rather than prudent rejection.	Contingency theory	Ait Lemqeddem & Chouay (2020); El Haiba & Maimoun (2024); Pérez-Calderón et al. (2025)

Source : Authors' synthesis.

4. Results : Cross-Cutting Synthesis

Table 5 crosses the main families of technology identified in Sections 3.2.1 to 3.2.4 with their contribution to internal audit, the governance risks they raise, the mitigation mechanisms proposed in the literature and the corresponding role of the auditor. It separates data analytics, automation and AI in the strict sense, following the distinction made in Section 3.2.1, and it adds AI systems as an object of audit.

Table 5: Technologies, contributions, governance risks, mitigation mechanisms and auditor's role

Technology	Contribution to internal audit	Governance risks	Mitigation mechanisms	Role of the auditor
Data analytics and continuous monitoring	Full-population testing; earlier detection; shift from periodic to continuous assurance	Data quality; false positives; over-reliance on dashboards	Data governance; documented tests; periodic validation of rules	Designs and interprets tests; challenges the data
Robotic process automation	Automation of rules-based tasks; consistency and completeness of routine controls	Errors replicated at scale; access rights; process drift	Inventory of bots; access control; change management	Specifies and supervises the rules
Machine learning and anomaly detection	Detection of unusual patterns; prediction of risks	Opacity; bias; data quality; automation bias	Model validation; explainability requirements; documentation; human override	Interprets alerts, validates findings, exercises judgment
Natural language processing and generative AI	Analysis of contracts, reports and correspondence; drafting support	Hallucination; confidentiality of data; vendor dependence	Grounding on organizational documents; data-handling rules; review of outputs	Reviews and remains accountable for every output
Retrieval-augmented and agentic systems	Coordinated multi-step tasks with limited human intervention	Autonomy; accountability dilution; thin evidence base	Defined limits of autonomy; logging; escalation rules	Supervises goals and boundaries
AI systems as audit object	Assurance over models, data and controls of the organization	Opacity; restricted access to vendor models; threats to objectivity	Model inventory; algorithmic audit lifecycle; access clauses; safeguards for objectivity	Audits design, testing and monitoring

Source: Authors' synthesis from Sections 3.2.1 to 3.2.4.

The synthesis also reveals four tensions that organize the debate. The first opposes efficiency to assurance quality: gains in speed and coverage do not automatically improve the reliability of conclusions (Fedyk et al., 2022; Kokina & Davenport, 2017). The second opposes augmentation to substitution and deskilling, an instance of the automation-augmentation paradox described for management more broadly (Raisch & Krakowski, 2021). The third opposes performance to explainability: the most accurate models are often the least interpretable (Burrell, 2016; Casper et al., 2024). The fourth opposes the speed of adoption to regulatory and organizational maturity (Ait Lemqeddem & Chouay, 2020; Tabassi, 2023). A further finding concerns the balance of the corpus: most items address AI as an audit tool, whereas fewer address AI as an audit object (Casper et al., 2024; Lehner et al., 2022; Raji et al., 2020; Verma et al., 2025).

5. Discussion and Implications

5.1 Theoretical Implications

The synthesis carries implications for theory and practice. Theoretically, the paper contributes to the literature by explicitly connecting three streams of scholarship that are often treated separately: organizational governance theory, internal audit research, and the emerging literature on AI governance. This integration highlights that AI's effect on internal audit cannot

ISSN: 2658-8455
Volume 7, Issue 13 (2026), pp. 678-701.
© Authors: CC BY-NC-ND
IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

be adequately understood through a purely technical lens; rather, it must be situated within the broader governance architecture of the organization, in which accountability, independence, and legitimacy are at stake (Charreaux, 1997; Munoko et al., 2020). Relative to earlier work, the contribution is threefold. Issa et al. (2016) and Kokina and Davenport (2017) map opportunities and research agendas for AI in auditing, Fedyk et al. (2022) document effects in audit firms and Lehner et al. (2022) examine ethical challenges; this paper adds an internal audit perspective, a dual tool-and-object view and an explicit governance framework with testable propositions.

The paper also refines agency theory. AI can reduce information asymmetries between the principals of the organization and its agents by enabling exhaustive, real-time analysis, but it creates a second layer of delegation: the auditor delegates analytical tasks to an algorithmic system whose internal logic, training data and updates the auditor cannot fully observe. Strictly speaking, an algorithm has no interests of its own, so the relationship is best read as an analogy rather than a literal agency relationship; yet the structure of the problem is similar. The parties are the auditor (and, behind the auditor, the board and the audit committee) and the algorithmic system with its developer or vendor; the information asymmetry concerns the model's logic, data and drift; the agency costs are the costs of validation and monitoring plus the residual loss from undetected model errors; and the control mechanisms are model validation, documentation, independent testing and a structured right of human override. Research on trust in AI (Glikson & Woolley, 2020) and on automation bias (Parasuraman & Manzey, 2010) specifies the behavioral conditions under which this second layer of delegation is well calibrated or not, which is formalized in P3.

Finally, complementing agency theory with neo-institutional and sociomaterial arguments helps explain why audit functions may adopt AI under legitimacy pressure without the corresponding governance (P2, P5), and why the same technology can produce different practices in different settings.

5.2 Managerial Implications by Actor

From a managerial standpoint, the review suggests several priorities for organizations seeking to integrate AI into their internal audit function responsibly. Table 6 differentiates them by actor and translates them into concrete measures; each tied to a proposition of Section 3.3.2.

Table 6 : Concrete measures by actor

Actor	Concrete measures	Linked propositions
Chief audit executive (head of internal audit)	Build an inventory of the AI tools used by the function and of the AI systems in the risk universe; require validation and documentation (purpose, data, tests, limits) of any model used in audit work; keep traceable working papers for AI-assisted procedures; define which findings require human confirmation; run a competency program in data analytics, AI literacy and algorithmic risk	P1, P2, P3
Audit committee	Approve the mandate for the use of AI and for assurance over AI; require periodic reporting on AI-related risks and model validation; protect independence by separating advisory work on AI design from later assurance, or by safeguarding objectivity	P2, P4
Senior management	Allocate budget and data infrastructure; assign an accountable owner to each AI system; grant internal audit access to models, documentation and vendor evidence through contractual clauses; set rules for data submitted to external models	P2, P4, P5
Regulators and standard setters (IIA, national bodies)	Translate principles into audit-specific guidance and competency frameworks; clarify expectations for assurance over AI; in public settings, align with data protection law and national oversight bodies; support the development and testing of maturity models	P2, P5

Source: Authors' synthesis from Sections 3.2, 3.3 and 4.

Regarding sequencing, a staged and context-sensitive approach to adoption, starting with data foundations and rules-based automation before predictive or agentic capabilities, is plausible for resource-constrained and public-sector environments such as Moroccan public establishments, and it is consistent with evidence that the benefits of digitalization depend on organizational and infrastructural maturity (Ait Lemqeddem & Chouay, 2020; El Haiba & Maimoun, 2024). However, no validated maturity model supports this sequence for AI in internal audit, and building and testing one is a research priority (Section 6).

A further managerial implication concerns auditor independence. Because the credibility of internal audit rests on its perceived objectivity, organizations should resist the temptation to treat AI outputs as self-validating; instead, governance arrangements should explicitly preserve auditors' capacity and professional obligation to challenge, question, and where necessary override algorithmic conclusions (Baldwin et al., 2006; Parasuraman & Manzey, 2010). This is particularly important in contexts characterized by weaker regulatory or institutional frameworks, where the absence of robust legal and normative structures can itself become a source of governance risk. Such contexts do not necessarily display lower trust in algorithmic outputs: weak oversight may equally favor uncontrolled adoption and over-reliance, so the direction of the effect needs empirical testing (Pérez-Calderón et al., 2025).

5.3 Regulatory and Normative Environment

The review suggests that professional standard-setters and regulators have an important role to play in closing the gap between the rapid pace of AI adoption and the comparatively slower development of tailored governance frameworks. While broad principles such as fairness, transparency, and accountability are increasingly embedded in international standards (e.g., ISO/IEC, 2023), the literature consistently points to a shortage of operational, audit-specific guidance capable of translating these principles into day-to-day practice (Anica-Popa et al., 2026). Addressing this gap through more detailed professional guidance, competency frameworks, and, eventually, empirically validated maturity models constitutes a priority for both practice and future research. Table 7 compares the main instruments relevant to internal audit.

Table 7: Normative and regulatory instruments relevant to internal audit and AI

Instrument	Nature	Scope	Relevance for internal audit	Limit
Global Internal Audit Standards (IIA, 2024)	Professional standards	Internal audit function	Frame the mandate, objectivity and resources, including technology	Not AI-specific
COSO Internal Control: Integrated Framework (2013) and Enterprise Risk Management (2017)	Voluntary frameworks	Internal control; enterprise risk	Reference for assessing controls over technology and for integrating risk with strategy	Not AI-specific
ISO/IEC 42001:2023	Certifiable management system standard	Organizations developing or using AI	Benchmark for auditing an AI management system	Voluntary; process-oriented
Regulation (EU) 2024/1689	Binding regulation with risk-based obligations	AI systems placed on or used in the EU market	Defines obligations (for example for high-risk systems) that audits of AI may need to test	Territorial scope; no direct force in Morocco
NIST AI RMF 1.0	Voluntary framework	AI risk management	Govern, map, measure and manage functions usable as audit criteria	Voluntary; not audit-specific
Law 09-08 (Morocco)	Binding national law	Processing of personal data	Constrains the data that audit teams may submit to AI tools	Not AI-specific; interpreted by the supervisory authority

Source : Authors' synthesis from IIA (2024), COSO (2013, 2017), ISO/IEC (2023), European Union (2024), Tabassi (2023) and Royaume du Maroc (2009).

ISSN: 2658-8455
Volume 7, Issue 13 (2026), pp. 678-701.
© Authors: CC BY-NC-ND
IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

The comparison shows that no instrument is at once binding and specific to internal audit, which leaves a gap that professional guidance must fill. For Moroccan public establishments, the framework applicable to AI rests mainly on data protection and public accountability rules; the authors did not identify an AI-specific instrument in force at the time of writing.

5.4 Risks, Counter-Arguments and Benefit-Risk Balance

The benefits described above must be weighed against risks that are often under-reported. Confidentiality comes first: audit files may contain personal, commercial or classified data, and submitting them to external generative models raises legal and contractual exposure (Section 3.2.5). Cybersecurity and vendor dependence follow, since AI services concentrate risk in a small number of providers (Tabassi, 2023). Implementation costs, including licenses, data engineering and skills, are substantial for resource-constrained functions, and the energy consumption of large models adds an environmental cost (Strubell et al., 2019). Professional responsibility also remains with the auditor: if stakeholders come to believe that AI delivers full-population assurance, the gap between expected and delivered assurance may widen, whereas accountability for the opinion cannot be delegated to a system (Lehner et al., 2022). Finally, deskilling and automation bias may erode the judgment on which the profession rests (Brown-Liburd et al., 2015; Parasuraman & Manzey, 2010).

These counter-arguments do not invalidate the case for AI in internal audit; they condition it. The net balance depends on the governance mechanisms described in P2 and on the context described in P5.

6. Conclusion, Limitations and Future Research Avenues

This paper has examined how artificial intelligence is transforming the internal audit function within the broader context of organizational governance. Building on organizational governance theory and internal audit scholarship, the paper first argued that internal audit can be understood as a regulatory mechanism whose effectiveness rests on its capacity to provide independent, reliable, and timely assurance. It then suggested that AI introduces both significant opportunities (broader analytical coverage, faster detection of anomalies and the potential for continuous, predictive auditing) and significant governance risks, including algorithmic opacity, data quality concerns, automation bias and the erosion of auditor independence if oversight mechanisms are not deliberately maintained. Treating AI both as an audit tool and as an audit object, the review integrates these elements in a conceptual framework and five propositions (Section 3.3).

Relative to existing syntheses, which focus on external audit, firm-level effects or ethical principles, the review's central contribution lies in its integration of governance and AI perspectives: rather than treating AI adoption in internal audit as a purely technical or operational matter, the paper positions it as a governance challenge requiring explicit attention to accountability structures, competency development, and human oversight. This framing is particularly relevant for public-sector and resource-constrained organizations, where structural and infrastructural constraints may condition the extent to which AI's theoretical benefits are realized in practice. For decision-makers, the implications differ by actor (Table 6): internal audit leaders should inventory and validate the models they use, audit committees should safeguard independence and mandate assurance over AI, senior management should secure data foundations and access to models, and standard setters and regulators, including the IIA and national bodies, should translate principles into audit-specific guidance.

Several limitations of this study should be acknowledged. First, as a narrative and integrative review, the paper does not follow a fully systematic search protocol, and although the search and selection are documented (Section 2), the number of records screened was not logged, so

the synthesis does not offer the replicability of systematic reviews. The selection may also be biased by the authors' interest in public-sector internal audit, and the coding was carried out by a single researcher, without a second coder or expert validation. Second, much of the underlying evidence, particularly regarding time savings, cycle-time reductions and adoption rates, derives from a still-limited and fast-evolving body of empirical studies, often concentrated in specific sectors (e.g., banking) or geographic contexts and, for the most recent items, in a small number of publications, with a heterogeneous mix of academic and professional sources. This constrains the generalizability of the findings. Third, the paper's conceptual framework, while grounded in established theory, has not been empirically tested; its five propositions (Section 3.3.2) on the relationships among AI capabilities, governance mechanisms, the auditor's role and internal audit effectiveness remain to be validated through primary data collection.

These limitations point directly to avenues for future research. Four research designs follow from the propositions. First, a survey of internal auditors in Moroccan public establishments and banks, analyzed with structural equation modeling, could test whether AI use is associated with coverage, detection, independence and quality of reporting (P1), whether governance mechanisms moderate this association (P2) and whether auditor oversight mediates it (P3). Second, multiple case studies of internal audit functions that audit AI systems could examine how model inventories, validation and access rights work in practice and where they fail (P4). Third, a Delphi study with internal audit leaders, audit committee members and regulators could validate the framework and develop a maturity model for staged AI adoption in resource-constrained public settings (P5). Fourth, controlled experiments could manipulate the reliability and explainability of algorithmic alerts to measure automation bias and its effect on auditors' independence judgments (P3). Beyond these designs, research is needed on how competency frameworks are evolving, on the implications of increasingly autonomous audit-support systems for professional judgment and accountability, and on how the very definition of independent assurance may change in an AI-driven organizational environment.

References

(1). Ait Lemqeddem, H., & Chouay, J. (2020). Le rôle de la digitalisation dans l'efficacité de l'audit interne. *Revue Française d'Économie et de Gestion, 1*(5), 48–65.

(2). Alami Gholami, E., & Lotfi, M. (2026). Artificial intelligence and the transformation of internal audit in the banking sector. *Revue Internationale des Sciences de Gestion, 9*(2), 639–650.

(3). Anica-Popa, I.-F., Tudor, C.-G., Anica-Popa, L.-E., & Vrîncianu, M. (2026). Reframing internal audit through emerging AI technologies: Toward an integration framework and assessment model. *Electronics*, *15*(11), Article 2280. https://doi.org/10.3390/electronics15112280

(4). Anthony, R. N., & Govindarajan, V. (2007). *Management control systems* (12th ed.). McGraw-Hill.

(5). 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

(6). Baldwin, A. A., Brown, C. E., & Trinkle, B. S. (2006). Opportunities for artificial intelligence development in the accounting domain: The case for auditing. *Intelligent Systems in Accounting, Finance and Management, 14*(3), 77–86. https://doi.org/10.1002/isaf.277

(7). Berle, A. A., & Means, G. C. (1932). *The modern corporation and private property*. Macmillan.

ISSN: 2658-8455
Volume 7, Issue 13 (2026), pp. 678-701.
© Authors: CC BY-NC-ND
IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

(8). Bhimani, A., & Willcocks, L. (2014). Digitisation, "Big Data" and the transformation of accounting information. *Accounting and Business Research, 44*(4), 469–490. https://doi.org/10.1080/00014788.2014.910051
(9). Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. *European Law Journal, 13*(4), 447–468. https://doi.org/10.1111/j.1468-0386.2007.00378.x
(10). Bresnahan, T. F., & Trajtenberg, M. (1995). General purpose technologies: "Engines of growth"? *Journal of Econometrics, 65*(1), 83–108. https://doi.org/10.1016/0304-4076(94)01598-T
(11). 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-51023
(12). Brynjolfsson, E., Rock, D., & Syverson, C. (2019). Artificial intelligence and the modern productivity paradox: A clash of expectations and statistics. In A. Agrawal, J. Gans, & A. Goldfarb (Eds.), *The economics of artificial intelligence: An agenda* (pp. 23–57). University of Chicago Press.
(13). Burrell, J. (2016). How the machine "thinks": Understanding opacity in machine learning algorithms. *Big Data & Society, 3*(1). https://doi.org/10.1177/2053951715622512
(14). Casper, S., Ezell, C., Siegmann, C., Kolt, N., Curtis, T. L., Bucknall, B., Haupt, A., Wei, K., Scheurer, J., Hobbhahn, M., Sharkey, L., Krishna, S., Von Hagen, M., Alberti, S., Chan, A., Sun, Q., Gerovitch, M., Bau, D., Tegmark, M., . . . Hadfield-Menell, D. (2024). Black-box access is insufficient for rigorous AI audits. In *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency* (pp. 2254–2272). Association for Computing Machinery. https://doi.org/10.1145/3630106.3659037
(15). Chan, D. Y., & Vasarhelyi, M. A. (2011). Innovation and practice of continuous auditing. *International Journal of Accounting Information Systems, 12*(2), 152–160. https://doi.org/10.1016/j.accinf.2011.01.001
(16). Charreaux, G. (Ed.). (1997). *Le gouvernement des entreprises: Corporate governance, théories et faits*. Economica.
(17). Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control: Integrated framework*. https://www.coso.org/guidance-on-ic
(18). Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance*. https://www.coso.org/guidance-erm
(19). Curtis, M. B., & Payne, E. A. (2008). An examination of contextual factors and individual characteristics affecting technology implementation decisions in auditing. *International Journal of Accounting Information Systems, 9*(2), 104–121. https://doi.org/10.1016/j.accinf.2007.10.002
(20). Davenport, T. H., & Ronanki, R. (2018). Artificial intelligence for the real world. *Harvard Business Review, 96*(1), 108–116.
(21). Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340. https://doi.org/10.2307/249008
(22). DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147–160. https://doi.org/10.2307/2095101
(23). Donaldson, L. (2001). *The contingency theory of organizations*. Sage.

(24). El Haiba, F., & Maimoun, A. (2024). L'impact de la digitalisation sur l'audit interne: Opportunités et défis à l'ère de la numérisation. *African Scientific Journal, 3*(22), 850–868.
(25). European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, L 2024/1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj
(26). Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022). Is artificial intelligence improving the audit process? *Review of Accounting Studies, 27*(3), 938–985. https://doi.org/10.1007/s11142-022-09697-x
(27). Freeman, R. E. (1984). *Strategic management: A stakeholder approach*. Pitman.
(28). Glikson, E., & Woolley, A. W. (2020). Human trust in artificial intelligence: Review of empirical research. *Academy of Management Annals, 14*(2), 627–660. https://doi.org/10.5465/annals.2018.0057
(29). Gramling, A. A., Maletta, M. J., Schneider, A., & Church, B. K. (2004). The role of the internal audit function in corporate governance: A synthesis of the extant internal auditing literature and directions for future research. *Journal of Accounting Literature, 23*, 194–244.
(30). Grant, M. J., & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal, 26*(2), 91–108. https://doi.org/10.1111/j.1471-1842.2009.00848.x
(31). Institute of Internal Auditors. (2024). *Global internal audit standards*. https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/
(32). Internal Audit Foundation, & Wolters Kluwer TeamMate. (2024). *Solving the riddle: Harnessing generative AI for internal audit activities*. https://www.theiia.org/globalassets/site/content/research/foundation/2024/harnessinggenerativeai_1.pdf
(33). International Organization for Standardization, & International Electrotechnical Commission. (2023). *Information technology: Artificial intelligence: Management system* (ISO/IEC Standard No. 42001:2023). https://www.iso.org/standard/81230.html
(34). 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
(35). Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics, 3*(4), 305–360. https://doi.org/10.1016/0304-405X(76)90026-X
(36). Kamareldawla, N. M. (2025). External auditors' perceptions toward the use of artificial intelligence in the audit process and ethical challenges facing its application: Evidence from an emerging market. *Corporate Ownership & Control, 22*(2), 171–184. https://doi.org/10.22495/cocv22i2art16
(37). 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
(38). Lehner, O. M., Ittonen, K., Silvola, H., Ström, E., & Wührleitner, A. (2022). Artificial intelligence based decision-making in accounting and auditing: Ethical challenges and normative thinking. *Accounting, Auditing & Accountability Journal, 35*(9), 109–135. https://doi.org/10.1108/AAAJ-09-2020-4934
(39). Lenz, R., & Hahn, U. (2015). A synthesis of empirical internal audit effectiveness literature pointing to new research opportunities. *Managerial Auditing Journal, 30*(1), 5–33. https://doi.org/10.1108/MAJ-08-2014-1072

ISSN: 2658-8455
Volume 7, Issue 13 (2026), pp. 678-701.
© Authors: CC BY-NC-ND

(40). 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
(41). Munoko, I., Brown-Liburd, H. L., & Vasarhelyi, M. (2020). The ethical implications of using artificial intelligence in auditing. *Journal of Business Ethics, 167*(2), 209–234. https://doi.org/10.1007/s10551-019-04407-1
(42). O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown.
(43). Orlikowski, W. J., & Scott, S. V. (2008). Sociomateriality: Challenging the separation of technology, work and organization. *Academy of Management Annals, 2*(1), 433–474. https://doi.org/10.1080/19416520802211644
(44). Ouhoud, O., & El Ouafa, K. (2025). Le rôle transformationnel de l'intelligence artificielle dans l'audit interne à l'ère du digital. *International Journal of Accounting, Finance, Auditing, Management and Economics, 6*(10), 560–578.
(45). Parasuraman, R., & Manzey, D. H. (2010). Complacency and bias in human use of automation: An attentional integration. *Human Factors, 52*(3), 381–410. https://doi.org/10.1177/0018720810376055
(46). Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management, 52*(2), 183–199. https://doi.org/10.1016/j.im.2014.08.008
(47). Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
(48). Pérez-Calderón, E., Alrahamneh, S. A., & Milanés Montero, P. (2025). Impact of artificial intelligence on auditing: An evaluation from the profession in Jordan. *Discover Sustainability, 6*, Article 251. https://doi.org/10.1007/s43621-025-01058-3
(49). Power, M. (1997). *The audit society: Rituals of verification*. Oxford University Press.
(50). Raisch, S., & Krakowski, S. (2021). Artificial intelligence and management: The automation–augmentation paradox. *Academy of Management Review, 46*(1), 192–210. https://doi.org/10.5465/amr.2018.0072
(51). Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (pp. 33–44). Association for Computing Machinery. https://doi.org/10.1145/3351095.3372873
(52). Reynaud, J.-D. (1989). *Les règles du jeu: L'action collective et la régulation sociale*. Armand Colin.
(53). Rezaee, Z., Sharbatoghlie, A., Elam, R., & McMickle, P. L. (2002). Continuous auditing: Building automated auditing capability. *Auditing: A Journal of Practice & Theory, 21*(1), 147–163. https://doi.org/10.2308/aud.2002.21.1.147
(54). Roberts, J., & Scapens, R. (1985). Accounting systems and systems of accountability: Understanding accounting practices in their organisational contexts. *Accounting, Organizations and Society, 10*(4), 443–456. https://doi.org/10.1016/0361-3682(85)90015-3
(55). Royaume du Maroc. (2009). *Dahir n° 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel*. Bulletin officiel n° 5714 du 23 février 2009.
(56). Royaume du Maroc. (2011). *Constitution du Royaume du Maroc (Dahir n° 1-11-91 du 27 chaabane 1432 [29 juillet 2011])*. Bulletin officiel n° 5964 bis du 30 juillet 2011.

(57). Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

(58). Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

(59). Strubell, E., Ganesh, A., & McCallum, A. (2019). Energy and policy considerations for deep learning in NLP. In *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics* (pp. 3645–3650). Association for Computational Linguistics. https://doi.org/10.18653/v1/P19-1355

(60). Tabassi, E. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1

(61). Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review, 4*(3), 356–367. https://doi.org/10.1177/1534484305278283

(62). 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

(63). Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478. https://doi.org/10.2307/30036540

(64). Verma, H., Padh, K., & Thelisson, E. (2025). Can AI be auditable? In M. Constantinides & D. Quercia (Eds.), *Operationalizing responsible AI: Opportunities and challenges*. Cambridge University Press.

(65). Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*(2), xiii–xxiii.

(66). Zhang, G., Atasoy, H., & Vasarhelyi, M. A. (2022). Continuous monitoring with machine learning and interactive data visualization: An application to a healthcare payroll process. *International Journal of Accounting Information Systems, 46*, Article 100570. https://doi.org/10.1016/j.accinf.2022.100570