ISSN: 2658-8455
Volume 7, Issue 10 (2026), pp. 366-381.

Artificial Intelligence in Financial Fraud Detection: A Conceptual Literature Review

Nouhad LAOUANE, *(PhD Student in Economics and Management)*
Faculty of Economics and Management (LARPEG)
Sultan Moulay Slimane University, Béni Mellal, Morocco.

Aya EL-GATRANI, *(PhD Student in Economics and Management)*
Faculty of Economics and Management (LARPEG)
Sultan Moulay Slimane University, Béni Mellal, Morocco.

Abdelhadi DARKAOUI, *(Professor - Researcher in Economics and Management)*
Faculty of Economics and Management (LARPEG)
Sultan Moulay Slimane University, Béni Mellal, Morocco.

Adresse de correspondance :	Faculté des Sciences Juridiques, Économiques et Sociales, Université Sultan Moulay Slimane, Béni Mellal, Maroc (LARPEG).
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	LAOUANE, N., EL-GATRANI, A., & DARKAOUI, A. (2026). Artificial Intelligence in Financial Fraud Detection: A Conceptual Literature Review. *International Journal of Accounting, Finance, Auditing, Management and Economics*, *7*(10), 366–381. https://doi.org/10.5281/zenodo.22167451
Licence	**Cet article est publié en open Access sous licence CC BY-NC-ND**

Received: 01/07/2026 *Accepted: 30/08/2026*

International Journal of Accounting, Finance, Auditing, Management and Economics - IJAFAME
ISSN: 2658-8455
Volume 7, Issue 10 (2026)

Artificial Intelligence in Financial Fraud Detection : A Conceptual Literature Review

Abstract

Artificial intelligence (AI) is increasingly applied to financial fraud detection in response to the growing complexity of fraudulent schemes and the exponential increase in data volumes. Despite abundant evidence of AI's technical performance, the literature has not yet proposed a model that simultaneously integrates its technological, organizational, and institutional dimensions: this is the gap the present theoretical research addresses. Based on an integrative review drawing mainly on studies published between 2009 and 2023 in auditing, information systems, and AI governance research, this strictly conceptual study draws on Agency Theory, the Resource-Based View, Institutional Theory, and the socio-technical systems approach to propose a model articulating five variables: AI adoption, data quality, institutional governance maturity, human-AI complementarity, and fraud detection performance. Four hypotheses posit that AI adoption influences detection performance both directly and indirectly, through two mediating mechanisms (data quality and human-AI complementarity), moderated by governance maturity. This model gives rise to a "Conditional Transformation Theory," in which each of these four hypotheses illustrates one condition of AI's partial, rather than revolutionary, transformation of financial control, contingent on the co-evolution of technological and institutional capabilities. Applied to the Moroccan context, viewed as an institutional transition laboratory, the study outlines directions for future empirical validation.

Keywords: Artificial Intelligence, Financial Fraud Detection, Management Control, Augmented Decision-Making, Digital Transformation, Audit Analytics.
Classification JEL: M42, G28, O33
Paper type: Theoretical Research

Résumé

L'intelligence artificielle (IA) occupe une place croissante dans la détection de la fraude financière, face à la complexification des pratiques frauduleuses et à l'explosion des volumes de données. Malgré l'abondance des travaux démontrant la performance technique de l'IA, la littérature ne propose pas encore de modèle intégrant simultanément ses dimensions technologique, organisationnelle et institutionnelle : c'est ce déficit que la présente recherche théorique se propose de combler. Sur la base d'une revue intégrative mobilisant principalement des travaux publiés entre 2009 et 2023 dans les domaines de l'audit, des systèmes d'information et de la gouvernance de l'IA, cette étude, de nature strictement conceptuelle, s'appuie sur la théorie de l'agence, la théorie des ressources, la théorie néo-institutionnelle et l'approche sociotechnique pour proposer un modèle articulant cinq variables : adoption de l'IA, qualité des données, maturité de la gouvernance institutionnelle, complémentarité humain-IA et performance de détection. Quatre hypothèses postulent que l'adoption de l'IA influence la performance de détection directement et indirectement, via un double effet médiateur (qualité des données, complémentarité humain-IA), sous l'effet modérateur de la maturité de la gouvernance. Ce modèle conduit à la théorie de la « transformation conditionnelle », selon laquelle chacune de ces quatre hypothèses illustre une condition de la transformation partielle, et non révolutionnaire, du contrôle financier par l'IA, subordonnée à la co-évolution des capacités technologiques et institutionnelles. Appliquée au contexte marocain, envisagé comme un laboratoire de transition institutionnelle, l'étude ouvre des perspectives de validation empirique future.

Mots clés : Intelligence artificielle, Détection de la fraude financière, Contrôle de gestion, Pilotage décisionnel augmenté, Transformation numérique, Audit analytique.
JEL Classification : M42, G28, O33
Type du papier : Recherche Théorique

ISSN: 2658-8455
Volume 7, Issue 10 (2026), pp. 366-381.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

1. Introduction

Over the past two decades, the digital transformation of economic and financial systems has profoundly reshaped the dynamics of financial information production, circulation, and security. The expansion of electronic payments, transaction platforms, digital financial services, and interconnected digital infrastructures has significantly improved the efficiency of economic exchanges. However, this transformation has been accompanied by a parallel evolution in financial fraud mechanisms, characterized by increasing sophistication, rapid adaptation to control mechanisms, and systematic exploitation of technological and organizational vulnerabilities. In this context, traditional financial control mechanisms primarily based on periodic reviews, sampling procedures, and static rule-based controls are progressively showing their limitations when confronted with massive, dynamic, and highly interconnected transaction environments.

In response to this growing complexity, Artificial Intelligence (AI) has emerged as a technological solution capable of redefining fraud detection practices. Machine learning techniques, predictive analytics, anomaly detection methods, and relational network analysis now enable the processing of data volumes that exceed the analytical capacity of traditional control methods. In institutional and professional discourse, AI is often presented as a disruptive innovation capable of enabling continuous, predictive, and automated financial control. However, this technology-driven perspective remains contested in academic literature, which increasingly emphasizes that the effectiveness of AI systems depends strongly on organizational, institutional, and human factors, including data quality, digital governance maturity, and the capacity of organizations to effectively integrate AI into decision-making processes.

Having situated Artificial Intelligence within this broader global movement of financial digitalization, it is useful to narrow the analysis to a specific institutional setting in which these dynamics can be more concretely examined. Emerging economies undergoing simultaneous digital and regulatory transitions offer a particularly instructive vantage point, as the institutional conditions surrounding AI adoption are often still forming rather than fully consolidated.

Within this context, Morocco represents a particularly relevant analytical environment for examining the institutional conditions shaping Artificial Intelligence adoption in financial control systems. The country is currently undergoing a dual transformation combining accelerated public sector digitalization and progressive strengthening of regulatory frameworks related to data governance, cybersecurity, and public financial accountability.

Rather than being approached as a purely descriptive national case, Morocco can be conceptualized as an institutional transition laboratory. In such environments, the effectiveness of Artificial Intelligence in financial fraud detection depends on the alignment between technological adoption capacity, governance maturity, data ecosystem structuring, and human capability development.

Similar to many emerging governance contexts, Morocco's digital transformation occurs within an institutional landscape characterized by heterogeneous digital maturity levels, uneven information system interoperability, and progressive but uneven development of data governance practices. This institutional heterogeneity provides a particularly relevant analytical setting for examining the conditions under which Artificial Intelligence can generate genuinely transformative effects in financial control systems. This institutional trajectory is illustrated, for example, by the adoption of Law No. 09-08 on the protection of individuals with regard to the processing of personal data and the ongoing supervisory role of the National Commission for the Control of Personal Data Protection (CNDP), as well as by the digital economy monitoring reports regularly published by the National Telecommunications Regulatory Agency (ANRT).

This research pursues three main objectives. First, it aims to develop a conceptual framework integrating technological, organizational, and institutional dimensions of AI adoption in financial control. Second, it proposes an analytical model designed to examine the relationships between AI adoption, governance maturity, data quality, and fraud detection performance. Third, it contributes to the literature by proposing a "conditional transformation" theoretical perspective, according to which the revolutionary impact of AI depends on the co-evolution of technological and institutional capabilities.
Building on these objectives, this research is guided by a central research question: under what institutional and organizational conditions does Artificial Intelligence adoption translate into effective financial fraud detection performance? The conceptual model and hypotheses developed in the following sections are designed to address this question.
The remainder of this article is organized as follows. Section 2 reviews the literature on financial fraud, AI-based detection, and institutional governance, before presenting the theoretical framework and the conceptual model. Section 3 details the methodological positioning of the research. Section 4 discusses the conceptual model in light of the reviewed literature. Section 5 develops the theoretical, managerial, and public governance implications. Section 6 outlines the limitations of the study and avenues for future research, and Section 7 concludes.

2. Literature Review and Theoretical Framework

2.1 Evolution of Financial Fraud and Transformation of Financial Control Systems

Financial fraud represents a structural phenomenon within economic systems, evolving in parallel with technological, organizational, and institutional transformations. The seminal work of Cressey (1953) introduced the Fraud Triangle concept, identifying pressure, opportunity, and rationalization as key determinants of fraudulent behavior. This framework was later expanded by Albrecht et al. (2012), who emphasized the increasing complexity of fraud mechanisms in modern organizational environments.
Contemporary empirical research demonstrates that the digital transformation of financial systems has fundamentally altered fraudulent operating models. According to reports from the Association of Certified Fraud Examiners (ACFE, 2022), financial fraud is increasingly linked to digital technologies, particularly through electronic payment systems, transactional platforms, and interconnected digital infrastructures.
The literature generally distinguishes several categories of financial fraud. Accounting fraud, widely studied in auditing and corporate governance research, involves the intentional manipulation of financial statements to conceal the true economic performance of an organization (Dechow et al., 2011). Transactional fraud refers to individual financial operations such as fraudulent payments and unauthorized transfers (Ngai et al., 2011). More recently, research has highlighted the emergence of cyber-enabled financial fraud, combining technical cyber methods with behavioral manipulation strategies (Kshetri, 2021).
In parallel, traditional financial control systems have historically relied on internal control frameworks, particularly the COSO framework (COSO, 2013), as well as risk-based auditing approaches. These mechanisms have demonstrated strong effectiveness in relatively stable transactional environments. However, several studies highlight their limitations in digital environments characterized by massive data volumes and real-time information flows (Power, 1997; Vasarhelyi et al., 2015).
Sampling-based approaches may be insufficient to detect rare but critical anomalies in big data environments. Moreover, rule-based control systems can be circumvented by adaptive fraud schemes. These limitations have driven the development of advanced analytical approaches based on large-scale data exploitation and artificial intelligence.

2.2 Artificial Intelligence and Financial Fraud Detection: State of Research

The emergence of Artificial Intelligence in accounting and auditing practices was first documented by Kokina and Davenport (2017), who identified its early applications in financial statement analysis and fraud-related tasks. This body of research can be read along a central tension: an initial, largely deterministic strand documenting AI's technical capabilities, contrasted with a more recent, critical strand emphasizing the organizational and data conditions under which these capabilities actually translate into performance. Recent research demonstrates that Artificial Intelligence represents a major driver of improvement in financial fraud detection capabilities. The work of Dai and Vasarhelyi (2020) on continuous audit intelligence and analytics highlights how automated analysis of large datasets enhances early anomaly detection.

Although a growing body of research highlights the technological superiority of Artificial Intelligence in fraud detection, the literature remains divided regarding the real transformational capacity of these technologies. Early research largely focused on the predictive power of machine learning algorithms and anomaly detection techniques (Ngai et al., 2011; Chandola et al., 2009). These studies demonstrate the capacity of AI models to identify hidden patterns within large financial datasets.

Machine learning algorithms enable the identification of complex correlations between transactional variables and fraudulent behaviors (Ngai et al., 2011). Appelbaum et al. (2017) show that integrating Artificial Intelligence into auditing processes significantly improves the detection of complex fraud schemes.

Deep learning research indicates that these models can identify complex non-linear structures in financial data (Craja et al., 2020). In addition, unsupervised anomaly detection systems allow the identification of unusual behavioral patterns in environments characterized by continuously evolving fraud strategies (Chandola et al., 2009).

Natural Language Processing enables the analysis of unstructured data such as financial documents and electronic communications (Brown-Liburd et al., 2015). Graph-based analytics supports the identification of complex fraud networks involving multiple actors (Weber et al., 2019).

However, more recent research adopts a more critical perspective. Several authors argue that the performance of AI systems is strongly dependent on data quality, data governance, and organizational implementation conditions (Mikalef et al., 2020; Munoko et al., 2020; Dwivedi et al., 2021). In particular, the presence of biased, incomplete, or poorly structured datasets may significantly reduce model reliability and increase false detection rates.

Furthermore, while AI systems are often presented as autonomous decision-making tools, socio-technical research emphasizes the continued importance of human expertise in fraud investigation processes. Human auditors remain essential for contextual interpretation, legal qualification of suspicious transactions, and final decision validation (Brown-Liburd et al., 2015).

In parallel, institutional research highlights that technology adoption is often driven not only by efficiency considerations but also by regulatory pressure and organizational legitimacy concerns (DiMaggio & Powell, 1983). This perspective suggests that AI adoption may sometimes be symbolic rather than transformational.

2.3 Governance, Institutional Maturity, and Artificial Intelligence Adoption

Recent literature emphasizes that Artificial Intelligence adoption depends not only on technological capabilities but also on the institutional maturity level of organizations. According to Mikalef et al. (2020), the value of data-driven analytical capabilities depends strongly on organizational capabilities and information infrastructure quality.

Research on AI governance highlights the importance of algorithmic transparency, model explainability, and regulatory compliance (Ransbotham et al., 2017; Dwivedi et al., 2021). In the public sector, these requirements are reinforced by accountability and institutional transparency principles.

Recent research also highlights the growing importance of Artificial Intelligence governance frameworks and ethical standards in ensuring responsible deployment of AI systems, particularly in public sector and financial control environments (Floridi et al., 2018; Jobin et al., 2019).

In institutional contexts undergoing transformation, the impact of Artificial Intelligence strongly depends on the ability of organizations to align technological transformation with organizational transformation. In such environments, the effectiveness of AI deployment is increasingly linked to the development of coherent governance frameworks, ethical oversight mechanisms, and institutional capacity building processes. It should be noted that this body of governance and AI-adoption literature remains, at this stage, predominantly anchored in North American, European, and global institutional settings. Recent Moroccan contributions nonetheless offer relevant contextual grounding for the institutional transition laboratory framing adopted in this article. Kassimi and Salam (2024) document the strategic, tactical, and operational dimensions of data governance within Moroccan public administration under the "Digital Morocco 2030" initiative, identifying persistent challenges such as the absence of a unified national data-governance strategy and recurring inter-institutional coordination gaps. Similarly, Belhaj and Boulahoual (2024), applying the OECD data-governance model to the Moroccan public sector, show that the country's data ecosystem is evolving but still requires stronger data infrastructure, interoperability, and human-capital development to fully support data-driven public value creation. More directly relevant to financial control specifically, Mabroumi and Aissaoui (2025) analyze the digital transformation of Morocco's public financial management systems - including the integrated expenditure management system (GID), the public procurement portal, and fiscal dematerialization - and find that governance and performance gains remain constrained by limited interoperability between institutions and uneven digital-skills capacity across ministries. These contributions confirm that Morocco's institutional environment combines an increasingly structured legislative and regulatory basis with unresolved coordination and infrastructural gaps, while also indicating that research specifically addressing AI governance in financial control remains comparatively scarce in the Moroccan and Maghreb context.

2.4 Theoretical Framework

The analysis of Artificial Intelligence in financial fraud detection is grounded in multiple complementary theoretical perspectives.

Agency Theory (Jensen & Meckling, 1976) explains financial fraud as a consequence of information asymmetries between economic actors. Artificial Intelligence can reduce these asymmetries by improving monitoring capabilities.

The Resource-Based View (Barney, 1991) considers Artificial Intelligence technologies as strategic resources whose value depends on their integration with existing organizational resources.

Institutional Theory (DiMaggio & Powell, 1983) explains that technology adoption can be influenced by regulatory, normative, and mimetic pressures.

Finally, the socio-technical systems approach (Trist, 1981; Bostrom & Heinen, 1977) highlights that technological system performance depends on alignment with organizational structures and human competencies.

These four theoretical perspectives are not simply juxtaposed but articulate distinct, sometimes tension-laden, logics of explanation. Agency Theory and the Resource-Based View share a

ISSN: 2658-8455
Volume 7, Issue 10 (2026), pp. 366-381.

rationalist premise, treating actors and resources as instruments of deliberate value creation, whereas Institutional Theory relativizes this rational agency by emphasizing that technology adoption may respond to legitimacy and conformity pressures rather than efficiency calculations alone. The socio-technical systems approach, for its part, cuts across this tension by insisting that neither purely rational resource allocation nor purely institutional conformity can, on its own, determine AI effectiveness: performance ultimately depends on the fit between technological systems and human-organizational structures. It is precisely this interplay of complementary and competing logics - efficiency-seeking, legitimacy-seeking, and structural fit - that the conditional transformation perspective proposed in this article seeks to capture, distinguishing it from conventional organizational contingency approaches, which typically model a single technology-context fit relationship without integrating institutional legitimacy dynamics.

From this integrated theoretical perspective, Artificial Intelligence can be interpreted as a conditional transformation factor in financial control, whose impact depends on the technological and institutional maturity levels of organizations.

2.5 Conceptual Research Model

Building on the literature review presented in the previous section, this research proposes a conceptual model designed to explain the conditions under which Artificial Intelligence (AI) contributes to improving financial fraud detection performance. While prior research has largely demonstrated the technical effectiveness of AI in fraud detection, relatively few studies have comprehensively examined the institutional and organizational conditions that influence the magnitude and sustainability of this impact.

The proposed conceptual model is based on the assumption that AI adoption alone does not automatically generate transformational effects in financial control systems. Instead, the effectiveness of AI depends on a broader organizational ecosystem including data quality, institutional governance maturity, and the integration of human expertise into AI-supported decision-making processes.

Within this framework, AI adoption is conceptualized as the primary technological driver of fraud detection capability. However, consistent with the Resource-Based View (Barney, 1991), the value of technological resources depends on their complementarity with organizational capabilities. In data-driven environments, data quality represents a strategic resource directly influencing AI model accuracy and reliability (Mikalef et al., 2020). In parallel, institutional governance maturity determines an organization's ability to deploy AI responsibly, ensuring transparency, accountability, and regulatory compliance (Dwivedi et al., 2021).

Furthermore, the socio-technical perspective suggests that technology effectiveness depends on the interaction between technological tools and human competencies (Trist, 1981). Therefore, the integration of human expertise is expected to enhance AI system performance by improving result interpretation, contextual decision-making, and investigation validation processes.

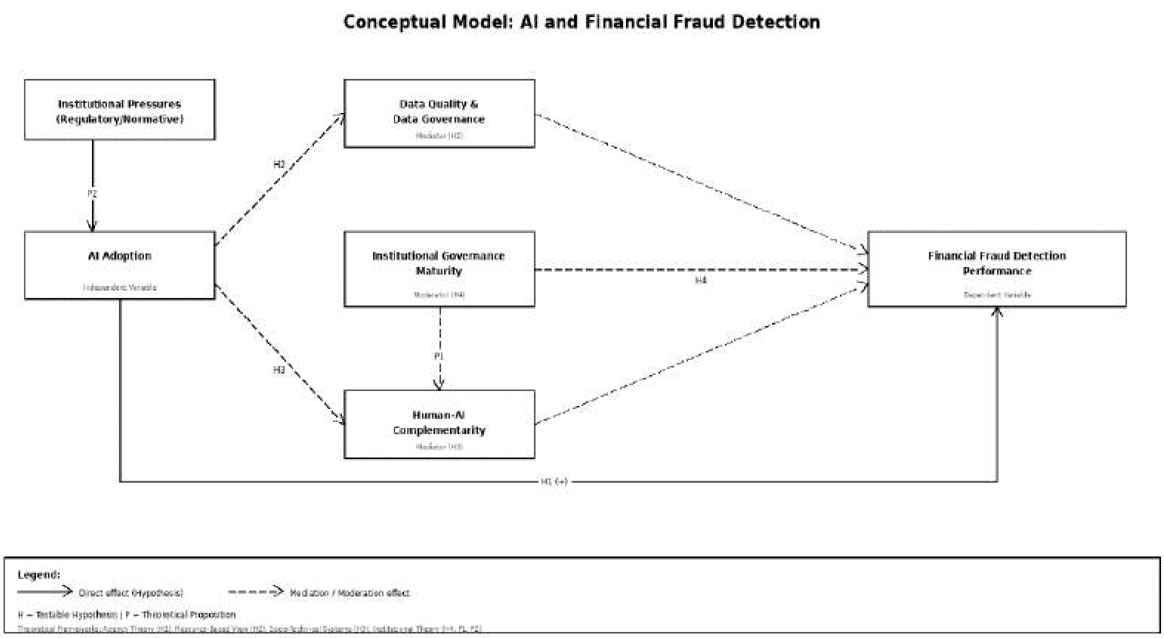
Accordingly, the proposed conceptual model assumes that AI adoption influences fraud detection performance both directly and indirectly through data quality and human-AI integration. In addition, institutional governance maturity is expected to moderate the relationship between AI adoption and fraud detection performance.

While a full-scale empirical validation lies beyond the scope of this conceptual article, a preliminary operationalization of the five constructs can guide future measurement efforts. AI adoption may be approached through the breadth and depth of AI-based tools deployed in fraud-detection processes (e.g., machine learning, anomaly detection, natural language processing). Data quality can be captured along accuracy, completeness, consistency, and timeliness dimensions, consistent with established data-quality frameworks. Institutional governance maturity may be assessed through the existence and enforcement of data-governance policies, algorithmic accountability mechanisms, and regulatory compliance structures. Human-AI complementarity can be operationalized through the degree of human oversight retained in AI-assisted decisions and the extent of collaborative validation between analysts and algorithmic outputs. Finally, fraud detection performance may be measured through indicators such as detection accuracy, false-positive rates, and detection latency. In addition to the moderating effect of governance maturity on the AI adoption-performance relationship, future research could also examine direct effects of governance maturity on data quality and on human-AI complementarity themselves, since stronger governance frameworks plausibly shape both the reliability of the data ecosystem and the conditions under which human-AI collaboration takes place.

2.6 Hypotheses and Theoretical Propositions Development

Artificial Intelligence enables the simultaneous analysis of large volumes of structured and unstructured financial data, facilitating real-time identification of complex fraud patterns. Several studies demonstrate that AI-based systems improve detection accuracy and reduce fraud detection time (Dai & Vasarhelyi, 2020; Appelbaum et al., 2017). From an Agency Theory perspective, improved monitoring capabilities reduce information asymmetries between organizational actors and strengthen internal control effectiveness (Jensen & Meckling, 1976).
H1: AI adoption positively influences financial fraud detection performance.
H2: Data quality mediates the relationship between AI adoption and financial fraud detection performance.
H3: Human-AI complementarity mediates the relationship between AI adoption and financial fraud detection performance.
H4: Institutional governance maturity positively moderates the relationship between AI adoption and financial fraud detection performance.
The proposed conceptual model is grounded in multiple theoretical perspectives, including Agency Theory, Resource-Based View, Institutional Theory, and Socio-Technical Systems Theory, and is supported by empirical findings from prior research on Artificial Intelligence adoption, data analytics performance, and AI governance in financial control systems.

Figure 1. Governance-Adjusted Conceptual Model of AI-Based Financial Fraud Detection Performance



Source: Authors, based on the literature review (2026)

ISSN: 2658-8455
Volume 7, Issue 10 (2026), pp. 366-381.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

As illustrated in Figure 1, the model assumes that Artificial Intelligence adoption directly influences financial fraud detection performance. However, this relationship is partially explained through two key mediating mechanisms: data quality and human-AI complementarity. Furthermore, institutional governance maturity moderates the strength of the relationship between Artificial Intelligence adoption and fraud detection performance. Figure 1 depicts these relationships schematically: a solid arrow represents the direct effect of AI adoption on fraud detection performance (H1); two parallel arrows passing through data quality and human-AI complementarity represent the two mediating paths (H2, H3); and a dotted arrow pointing toward the AI adoption-performance path represents the moderating effect of institutional governance maturity (H4).

3. Research Methodology

3.1 Methodological Positioning and Research Design

The choice of a conceptual approach is justified by the emerging nature of the phenomenon under investigation. The integration of Artificial Intelligence into financial control systems represents a rapidly evolving research field characterized by simultaneous transformations in technologies, organizational practices, and regulatory frameworks. In this context, several scholars emphasize the need to develop conceptual frameworks capable of structuring the understanding of technological transformations prior to conducting large-scale empirical investigations.

3.2 Epistemological Positioning

From an epistemological perspective, this research is grounded in a moderate positivist paradigm. The study assumes that organizational phenomena related to Artificial Intelligence adoption can be analyzed through theoretically grounded causal relationships.
This research relies on an integrative conceptual analysis combining critical literature review and theoretical structuring. The objective is to identify both convergences and divergences within existing scientific research related to Artificial Intelligence, data governance, audit analytics, and financial fraud detection.
The adopted approach consists of:
- Identifying key concepts mobilized in scientific literature
- Analyzing existing theoretical relationships between these concepts
- Proposing an integrative conceptual model
- Developing coherent explanatory hypotheses

This approach makes it possible to move beyond purely technological perspectives by incorporating organizational, human, and institutional dimensions. This methodological choice follows established guidance on integrative literature reviews, which emphasizes the deliberate combination of critical synthesis and theoretical structuring as a legitimate strategy for advancing conceptual knowledge in emerging research fields (Torraco, 2016).
The scientific corpus mobilized in this research is based on academic publications from auditing, information systems, Artificial Intelligence governance, and financial control research domains.
The sources include:
- Academic articles published in international scientific journals
- Foundational theoretical works in governance and organizational theory
- Recent empirical research on Artificial Intelligence applied to auditing and fraud detection
- Institutional reports related to Artificial Intelligence governance and digital transformation

This diversity of sources ensures a multidisciplinary understanding of the phenomenon under investigation.

The construction of the conceptual model is based on the identification of five key variables derived from existing literature:
- Artificial Intelligence adoption
- Data quality
- Institutional governance maturity
- Human-Artificial Intelligence complementarity
- Financial fraud detection performance

The relationships between these variables were established based on theoretical frameworks and empirical findings identified in prior literature.
To enhance the methodological transparency of this integrative review, relevant works were identified primarily through academic databases such as Scopus and Web of Science, using combinations of keywords including artificial intelligence, financial fraud detection, audit analytics, data governance, and institutional theory. The temporal coverage of the reviewed literature spans 1953 to 2023, with foundational theoretical works (fraud theory, agency theory, the resource-based view, institutional theory, and socio-technical systems theory) anchoring the earlier part of this range and AI-specific and AI-governance research concentrated between 2009 and 2023. Sources were included if they were peer-reviewed journal articles or foundational scholarly books directly addressing artificial intelligence, financial fraud, audit analytics, institutional governance, or one of the four theoretical frameworks mobilized in this article (agency theory, the resource-based view, institutional theory, and the socio-technical systems approach); non-peer-reviewed sources, conference abstracts without accessible full text, and publications not available in English or French were excluded. The corpus mobilized in this research comprises 27 references spanning the period 1953-2023. Approximately 15 of these were published from 2015 onward and directly address Artificial Intelligence, data analytics, or AI governance, while the remaining works constitute foundational theoretical contributions - fraud theory, agency theory, the resource-based view, institutional theory, and socio-technical systems theory - mobilized to ground the conceptual model rather than to document recent empirical findings on AI.
It should also be acknowledged, at this methodological stage, that a non-systematic conceptual review inherently involves a degree of interpretive judgment in the selection and articulation of sources. This subjectivity is mitigated, though not eliminated, by the explicit theoretical anchoring of the review and by the cross-referencing of convergent and divergent findings across the mobilized literature; this limitation is further discussed in Section 6.

3.3 Scientific Validity and Conceptual Robustness

The scientific validity of the proposed model is supported by multiple complementary dimensions. First, theoretical validity is ensured through the anchoring of the model in well-established theoretical frameworks. Second, conceptual validity relies on the internal consistency of the model and the compatibility of proposed relationships with existing empirical findings. Third, analytical validity is ensured through logical coherence between the literature review, theoretical framework, and conceptual model. These forms of validity are operationalized through three concrete criteria: the triangulation of multiple theoretical and empirical sources for each proposed relationship, the confrontation of the proposed model with competing theoretical frameworks (notably alternative contingency approaches), and an internal cross-reading of the manuscript aimed at identifying unsupported or overly generalized claims.

3.4 Ethical Considerations

This research complies with scientific integrity principles, including methodological transparency, analytical rigor, and scientific neutrality. The scientific works mobilized are cited according to academic standards, and the interpretations proposed are based on rigorous critical

ISSN: 2658-8455
Volume 7, Issue 10 (2026), pp. 366-381.

IJAFAME
International Journal of Accounting, Finance, Auditing, Management & Economics

analysis. As with any non-systematic literature review, a potential selection bias cannot be entirely excluded, since the choice of theoretical lenses and sources inevitably reflects the authors' disciplinary background and research priorities. This risk is partly mitigated by the deliberate inclusion of critical and contrasting perspectives throughout the review, rather than a purely confirmatory reading of the literature.

4. Discussion and Analytical Interpretation

4.1 Interpretation of the Conceptual Model

The conceptual model developed in this study provides a structured framework for understanding the mechanisms through which Artificial Intelligence contributes to financial fraud detection performance. While prior research has largely emphasized the technical superiority of AI-based detection systems, the findings of this conceptual analysis suggest that the impact of AI is contingent upon a broader organizational and institutional ecosystem.

4.2 AI in Financial Fraud Detection: Revolution or Controlled Transformation?

The findings of this research challenge the binary interpretation of Artificial Intelligence as either a revolutionary or purely incremental technological development. Instead, the results support a conditional transformation perspective, suggesting that the impact of AI depends on the interaction between technological capabilities and institutional readiness conditions.

4.3 The Role of Governance and Institutional Readiness

Building on the institutional dynamics discussed in Section 2.3, institutional readiness operates in this model specifically through its moderating role (H4): it is not adoption per se, but the depth of organizational integration behind it, that determines whether AI adoption translates into detection performance gains rather than symbolic compliance.
Governance maturity affects multiple dimensions of AI effectiveness, including data governance practices, algorithmic accountability, and regulatory alignment. Organizations with strong governance structures are better positioned to implement AI responsibly and sustainably. This convergent reading should nonetheless be nuanced. Several studies caution that AI-based detection systems can underperform, or even introduce new risks, in organizational contexts marked by weak data infrastructures or limited digital governance capacity (Mikalef et al., 2020), and institutional research similarly warns that AI adoption may remain largely symbolic when it is driven primarily by legitimacy pressures rather than genuine operational integration (DiMaggio & Powell, 1983). These more critical findings are consistent with, rather than contradictory to, the conditional transformation perspective: they illustrate precisely the boundary conditions under which AI fails to generate the anticipated gains.

4.4 Data Ecosystem Maturity and AI Effectiveness

Consistent with the data-quality mechanisms discussed in Section 2.2, data ecosystem maturity operates in this model as one of the two mediating paths (H2): it is through the reliability of the underlying data that AI adoption is expected to produce measurable gains in detection performance, rather than through adoption volume alone.
Data quality is therefore not only a technical issue but also a governance issue. Effective data governance requires organizational policies, accountability structures, and cross-functional coordination.
An illustrative case from the audit and compliance field lends secondary empirical support to this argument: several banking institutions' publicly reported partnerships with cloud-based AI providers for anti-money-laundering monitoring have been described in the financial press as delivering meaningful gains in detection coverage only once accompanied by substantial data-

cleansing and governance investments, underscoring that AI performance in fraud-related tasks is contingent on the surrounding data ecosystem rather than automatic.

4.5 Human Expertise and AI Complementarity

As anticipated by the human-AI complementarity mediating path (H3) and consistent with the socio-technical perspective developed in Section 2.2, full automation appears neither realistic nor desirable: it is the combination of algorithmic detection and human contextual judgment, rather than either in isolation, that the proposed model treats as a condition of effective fraud detection performance.

4.6 Toward a Conditional Transformation Theory

Based on the analysis, this research proposes the Conditional Transformation Theory of AI in financial control. According to this perspective, AI becomes transformative only when supported by strong governance frameworks, high-quality data ecosystems, and effective human-AI integration.

Conditional Transformation Theory departs from established socio-technical contingency approaches (Trist, 1981; Bostrom & Heinen, 1977) in two respects. First, whereas classical contingency models chiefly examine the fit between a technology and a single organizational context, the present framework treats institutional legitimacy dynamics, drawn from Institutional Theory, as a condition in its own right, distinct from purely technical or organizational fit. Second, the theory explicitly positions governance maturity as a variable that can shape the very mechanisms - data quality and human-AI complementarity - through which AI adoption produces its effects, rather than treating context as a single undifferentiated moderator. It is this dual conditionality, technical-organizational and institutional-legitimating, that distinguishes the proposed perspective from earlier contingency frameworks.

5. Theoretical, Managerial, and Public Governance Implications

5.1 Theoretical Implications

This research contributes to the academic literature by proposing a renewed perspective on the role of Artificial Intelligence in transforming financial control systems. While many studies present Artificial Intelligence as an inherently revolutionary transformation driver, this study highlights the contextual and conditional nature of its organizational impact.

First, this research contributes to the literature on Artificial Intelligence governance by demonstrating that AI system performance strongly depends on data ecosystem maturity and institutional structures. This perspective moves beyond purely technological analyses by integrating organizational and institutional dimensions of AI adoption.

Second, this research contributes to the evolution of the Resource-Based View by confirming that Artificial Intelligence technologies do not inherently constitute sustainable sources of organizational advantage. Their value depends on their combination with complementary resources such as data quality, human expertise, and organizational governance capabilities.

Third, this research reinforces the application of Institutional Theory in the field of emerging technology adoption. The findings suggest that AI adoption in financial control systems is influenced not only by operational efficiency considerations but also by regulatory, normative, and mimetic pressures.

Finally, this research contributes to socio-technical literature by demonstrating that Artificial Intelligence system performance strongly depends on the integration of human expertise into decision-making processes.

5.2 Managerial Implications

The results of this research suggest that organizations must adopt a systemic approach when integrating Artificial Intelligence into financial fraud detection systems. Technological investment alone is insufficient to generate sustainable performance improvements.

5.3 Public Governance Implications

In the public sector, the integration of Artificial Intelligence into financial control systems requires robust governance frameworks capable of balancing technological innovation with institutional accountability.
Public institutions must develop national Artificial Intelligence governance strategies integrating data governance, algorithmic regulation, and citizen rights protection.

5.4 Regulatory and Public Policy Implications

The findings of this research suggest that regulatory frameworks must evolve to address the specific characteristics of Artificial Intelligence systems. Regulators must develop standards for algorithmic transparency, automated decision explainability, and AI risk management. The European Union's Artificial Intelligence Act (European Parliament and Council of the European Union, 2024), which establishes a risk-based regulatory framework for AI systems, illustrates the type of regulatory architecture that could inform emerging governance contexts such as Morocco's. This regulatory challenge is compounded by the rapid diffusion of generative AI and large language models into financial services, which Lee et al. (2024) show already extends to fraud-related and compliance-related tasks, raising governance questions that go beyond the predictive and anomaly-detection systems primarily considered in the present conceptual model.
Public policies should also support the development of national data ecosystems capable of fostering innovation while ensuring the protection of sensitive data.

5.5 Financial Sovereignty in the Artificial Intelligence Era

The integration of Artificial Intelligence into financial control systems raises critical financial sovereignty issues. Public and financial organizations must maintain control over technological infrastructures and strategic data assets to limit external technological dependencies.
In this context, the development of national capabilities in Artificial Intelligence and data governance represents a strategic priority for financial security and institutional stability.

6. Limitations and Future Research

6.1 Research Limitations

Despite its theoretical and conceptual contributions, this research presents several limitations that should be acknowledged to ensure a balanced and rigorous scientific interpretation of the findings.
First, this study adopts a conceptual research design rather than an empirical validation approach. While conceptual models are essential for structuring emerging research fields, the absence of empirical testing limits the ability to statistically validate the proposed relationships. The conceptual nature of this research reflects the early-stage evolution of Artificial Intelligence integration into financial control ecosystems, particularly in emerging governance contexts. However, future empirical studies are necessary to test the proposed hypotheses and validate the conditional transformation framework.
Second, this research relies primarily on secondary academic and institutional sources. Although these sources provide strong theoretical and analytical grounding, they may not fully

capture the operational realities of AI implementation in specific institutional contexts. The gap between theoretical AI potential and practical implementation remains a challenge, particularly in complex public sector environments.

Third, the research adopts a global analytical perspective while integrating insights relevant to emerging governance contexts. However, institutional diversity across countries and public financial control systems may limit the generalizability of the proposed conceptual framework. Differences in regulatory environments, digital infrastructure maturity, data governance standards, and institutional capacity may produce heterogeneous AI adoption outcomes.

Fourth, the research focuses primarily on governance maturity, data quality, and human-AI complementarity as key explanatory factors. While these variables are strongly supported in existing literature, other factors such as organizational culture, cybersecurity maturity, vendor dependency risks, and political governance dynamics may also influence AI adoption and performance outcomes.

Fifth, the rapid technological evolution of Artificial Intelligence may affect the long-term stability of conceptual models. Advances in explainable AI, federated learning, and autonomous decision-making systems may alter the relationship between technology, governance, and human expertise over time.

6.2 Directions for Future Research

Future research should focus on empirical validation of the conceptual relationships proposed in this study. Quantitative research designs could test the proposed hypotheses across multiple institutional contexts. Survey-based studies targeting financial controllers, auditors, and public sector decision-makers could provide valuable empirical insights into AI adoption maturity and fraud detection performance outcomes.

Among these avenues, priority could reasonably be given to the Moroccan banking sector and to public financial-control institutions, given their advanced digitalization efforts and their direct exposure to the governance and data-quality conditions discussed in this article. A first empirical step could involve a survey-based test of the proposed hypotheses among bank compliance officers and internal auditors within an eighteen-to-twenty-four-month horizon, followed by comparative extensions to other public-sector financial-control bodies.

6.3 Toward Empirical Operationalization of Conditional Transformation Theory

Future studies could operationalize the conditional transformation framework by developing measurement scales for governance maturity, data ecosystem quality, and human-AI integration. Empirical testing of these constructs would strengthen the theoretical robustness and practical applicability of the model.

7. Conclusion

This study set out to critically examine the role of Artificial Intelligence in financial fraud detection, with the objective of determining whether its diffusion constitutes a paradigmatic revolution in financial control systems or a gradual technological extension of pre-existing control architectures. By mobilizing an integrative conceptual approach grounded in a critical literature review and a structured theoretical framework, the research demonstrates that the transformative effects of Artificial Intelligence are neither uniform nor deterministic, but instead deeply contingent upon organizational and institutional conditions.

In direct answer to the research question guiding this study, Artificial Intelligence adoption translates into effective financial fraud detection performance only when it is accompanied by sufficient data quality, mature institutional governance, and genuine human-AI complementarity - the conditions formalized in hypotheses H1 to H4 and synthesized in the Conditional Transformation Theory proposed here.

The analysis confirms that Artificial Intelligence holds considerable potential to reshape financial fraud detection through its capacity for real-time processing of large-scale financial data, advanced pattern recognition, and predictive risk modeling. These capabilities significantly expand the analytical boundaries of traditional financial control tools. However, the translation of this technological potential into structural transformation remains conditional. Its effectiveness is critically mediated by governance maturity, the coherence and quality of data infrastructures, and the degree of functional complementarity between algorithmic systems and human judgment within control processes.
From a theoretical perspective, and without repeating the detailed contributions already presented in Section 5, this research's central theoretical contribution is twofold: an integrative model linking AI adoption, governance maturity, data quality, and human-AI complementarity to fraud detection performance, and the conditional transformation perspective itself, which offers a more nuanced alternative to technologically deterministic narratives.
This research demonstrates that Artificial Intelligence represents a powerful yet contingent driver of transformation in financial fraud detection systems. Its impact is shaped less by technological sophistication per se than by the dynamic interaction between technology, institutional structures, organizational capabilities, and human expertise. By moving beyond reductionist and deterministic interpretations, this study offers a more robust and theoretically grounded understanding of the digital transformation of financial control systems and provides a foundation for future empirical and conceptual research in this field.

Références

(1). Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2012). Fraud examination (4th ed.). Cengage Learning.
(2). Appelbaum, D., Kogan, A., & Vasarhelyi, M. (2017). Analytics and artificial intelligence in auditing: Opportunities and challenges. International Journal of Accounting Information Systems, 26, 1-11.
(3). Association of Certified Fraud Examiners (ACFE). (2022). Report to the Nations: Global study on occupational fraud and abuse. ACFE.
(4). Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99-120.
(5). Belhaj, Y., & Boulahoual, A. (2024). La gouvernance des données au service de la création de valeur publique : Cas du Maroc. African Scientific Journal, 3(23), 635.
(6). Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. MIS Quarterly, 1(3), 17-32.
(7). Brown-Liburd, H., Issa, H., & Lombardi, D. (2015). Behavioral implications of big data in auditing. Accounting Horizons, 29(2), 143-154.
(8). Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1-58.
(9). Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). Internal control: Integrated framework. COSO.
(10). Craja, P., Kim, A., & Lessmann, S. (2020). Deep learning for detecting financial statement fraud. Decision Support Systems, 139, 113421.
(11). Cressey, D. R. (1953). Other people's money: A study in the social psychology of embezzlement. Free Press.
(12). Dai, J., & Vasarhelyi, M. A. (2020). Continuous audit intelligence as a service (CAIaaS) and intelligent app recommendations. Journal of Emerging Technologies in Accounting, 17(2), 1-15.
(13). Dechow, P. M., Ge, W., Larson, C., & Sloan, R. G. (2011). Predicting material accounting misstatements. Contemporary Accounting Research, 28(1), 17-82.

(14). 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.

(15). Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., ... Williams, M. D. (2021). Artificial intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and research agenda. International Journal of Information Management, 57, 101994.

(16). European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.

(17). Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... Vayena, E. (2018). AI4People: An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28(4), 689-707.

(18). 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.

(19). Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1(9), 389-399.

(20). Kassimi, Ouadih, & Salam, Ghizlane (2024). Gouvernance des données dans l'administration publique marocaine : Défis et perspectives. International Journal of Accounting, Finance, Auditing, Management and Economics, 5(12), 768-788.

(21). Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence in accounting. Journal of Emerging Technologies in Accounting, 14(1), 115-122.

(22). Kshetri, N. (2021). Cybercrime and cyber-enabled financial fraud: Implications for financial institutions. Journal of Financial Crime, 28(1), 182-198.

(23). Lee, D. K. C., Guan, C., Yu, Y., & Ding, Q. (2024). A comprehensive review of generative AI in finance. FinTech, 3(3), 460-478.

(24). Mabroumi, H., & Aissaoui, A. (2025). La transformation digitale des finances publiques au Maroc : enjeux de gouvernance et défis de performance. International Journal of Applied Management and Economics, 2(17), 293-308. https://doi.org/10.5281/zenodo.17979880

(25). Mikalef, P., Boura, M., Lekakos, G., & Krogstie, J. (2020). Big data analytics capabilities and firm performance: The mediating role of dynamic capabilities. Information & Management, 57(2), 103169.

(26). 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.

(27). Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559-569.

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

(29). Ransbotham, S., Kiron, D., Gerbert, P., & Reeves, M. (2017). Reshaping business with artificial intelligence: Closing the gap between ambition and action. MIT Sloan Management Review, Special Report, 1-17.

(30). Torraco, R. J. (2016). Writing integrative literature reviews: Using the past and present to explore the future. Human Resource Development Review, 15(4), 404-428.

(31). Trist, E. (1981). The evolution of socio-technical systems. Occasional Paper, Ontario Ministry of Labour.

(32). Vasarhelyi, M. A., Kogan, A., & Tuttle, B. (2015). Big data in accounting: An overview. Accounting Horizons, 29(2), 381-396.

(33). Weber, M., Domeniconi, G., Chen, J., Weidele, D. K. I., Bellei, C., Robinson, T., & Leiserson, C. E. (2019). Anti-money laundering in Bitcoin: Experimenting with graph convolutional networks for financial forensics. KDD Workshop on Anomaly Detection in Finance, arXiv:1908.02591.