IJOA.

AI and Information Systems Governance: Towards a Revision of Traditional Frameworks

Brahim KHIZRANE
b.khizrane.ced@uca.ac.ma
Laboratoire de Modélisation des
Systèmes Complexes ENSA, Maroc

Ahmed OUQOUR
ouqour.ahmed@eheec.ac.ma
Laboratoire Technologies et
Innovations Numériques HEEC, Maroc

Adnane LATIF
a.latif@uca.ac.ma
Laboratoire de Modélisation des
Systèmes Complexes ENSA, Maroc

Abstract—

The widespread adoption of artificial intelligence (AI) in organizations—estimated at 50% according to the McKinsey Global Institute (2023) [1]—is profoundly transforming information systems (IS) and their governance mechanisms. While traditional frameworks such as COBIT [2], ITIL [3], or ISO standards [4][5] provide robust foundations, they reveal significant limitations when confronted with AI-specific challenges, including the lack of integration of ethical dimensions [6][7][8], insufficient explainability of algorithmic decisions [9][10], unclear accountability in case of failure [11][12], and governance cycles too slow to keep pace with the exponential rate of innovation [13].

As emphasized by Floridi, Cowls, and Taddeo (2023) [17], European AI governance now places stronger emphasis on transparency, traceability, and algorithmic accountability, complementing traditional frameworks such as ISO and COBIT. Recent trends identified by Gartner (2024) [18] also confirm that organizational maturity in AI governance depends on the ability to automate compliance and to embed continuous feedback loops within management frameworks.

To analyze these issues, this research combines an extensive review of academic and professional literature with case studies of two multinational organizations: Amazon, which faced gender bias in its recruitment system [14], and Apple Card, in partnership with Goldman Sachs, which encountered bias in its credit scoring models [10][15]. The analysis highlights that current frameworks are insufficient to manage AI-specific risks and require adjustments at strategic, tactical, and operational levels.

The main contribution of this study lies in proposing a hybrid governance model integrating innovative mechanisms—such as the fusion of IS/AI governance committees, AI centers of excellence, and MLOps practices [16]—to ensure a more agile, transparent, and ethical governance approach.

Keywords—**Artificial Intelligence; IT Governance; Frameworks; Algorithmic Ethics; COBIT; Organizational Transformation.**

XII. INTRODUCTION

Artificial intelligence (AI) is now emerging as a major driver of organizational transformation, with an estimated adoption rate of 50% among companies according to McKinsey (2023) [1]. Its integration into areas such as finance, logistics, and human resources is reshaping information systems (IS) and putting their governance mechanisms to the test [3][6][7].

Traditional frameworks—COBIT [2], ITIL [3], and ISO standards [4][5]—provide a solid foundation but reveal significant limitations when confronted with the specificities of AI: insufficient integration of ethical dimensions [6][8], difficulties in explaining complex models [9][10], unclear responsibilities in the event of failure [11][12], and evolution cycles that are too slow [13][16]. As shown by Floridi, Cowls, and Taddeo (2023) [17], European AI governance now emphasizes transparency, traceability, and algorithmic accountability, thereby complementing traditional frameworks such as ISO and COBIT.

Recent trends identified by Gartner (2024) [18] confirm that organizational maturity in AI governance depends on the ability to automate compliance and integrate continuous feedback loops into management frameworks.

The cases of Amazon and Apple Card, marked by algorithmic biases in recruitment and credit allocation respectively [14][10][15], provide concrete illustrations of these shortcomings. This raises the central question: how can IS governance frameworks be adapted to maximize the value of AI while effectively managing its risks?

XIII. CONTEXT AND PROBLEM STATEMENT

AI now represents a lever of organizational transformation comparable to the advent of the Internet in the 1990s or cloud computing in the 2010s [3][6]. It is being integrated into a wide range of business processes—logistics, finance,

healthcare, and human resources—profoundly reshaping information systems (IS) governance [1].

However, this accelerated diffusion gives rise to specific risks:

• Bias and discrimination in automated decision-making [14][10].

• Opacity of models, making explainability difficult [9].
• Grey areas regarding responsibility in the event of system failure [11][12].

• A mismatch between the rapid evolution of technologies and the slow pace of normative and regulatory processes [13][16].

As a result, the central question becomes: how can IS governance frameworks be adapted to capture the value of AI without suffering from its ethical, technical, and legal pitfalls? [6][7][16].

As demonstrated by Floridi, Cowls, and Taddeo (2023) [17], European AI governance now places emphasis on transparency, traceability, and algorithmic accountability, thereby complementing traditional frameworks such as ISO and COBIT.

XIV. Methodology

III.1 LITERATURE REVIEW

An in-depth analysis of academic and professional contributions was conducted:

• **Academic research** (Brynjolfsson & McAfee [3], Jobin et al. [6], Raji et al. [10]) on the organizational and ethical impacts of AI. As shown by Floridi, Cowls, and Taddeo (2023) [17], European AI governance now emphasizes transparency, traceability, and algorithmic accountability, complementing traditional frameworks such as ISO and COBIT.

• **Institutional publications** (Accenture [9], OECD [7], UNESCO [8]) highlighting responsible governance and emerging regulation (AI Act [12]). The World Economic Forum (2024) [20] also stresses that AI governance must be supported by global audit and transparency frameworks, while the European Data Protection Board (2025) [19] emphasizes the compatibility between data protection and algorithmic governance.

III.2 CASE STUDIES

To concretely illustrate the limitations of governance frameworks when confronted with the specificities of AI, two emblematic cases were analyzed: Amazon and Apple Card.

III.2.1 AMAZON – GENDER BIAS IN RECRUITMENT

In 2018, Amazon abandoned a machine-learning-based recruitment tool after discovering that it systematically penalized female candidates in technical fields [14]. The algorithm, trained on historical data dominated by male profiles, reproduced and amplified gender discrimination.
• **Ethical risk:** violation of the principle of equal opportunity, negatively affecting diversity and inclusion.
• **Organizational risk:** loss of credibility and reputational damage, with Amazon heavily criticized for failing to anticipate bias.
• **Link to IS governance:** absence of algorithmic auditability mechanisms in traditional frameworks (COBIT, ITIL) [2][3], which do not explicitly address bias detection and correction.

III.2.2 APPLE CARD – BIAS IN CREDIT SCORING

Apple Card faced bias in its credit-scoring models, disadvantaging certain customer categories [10][15][15]. These biases, stemming from socio-economic data, called into question the fairness and transparency of the decision-making process.

• **Regulatory risk:** potential non-compliance with anti-discrimination and consumer protection regulations [12].

• **Technical risk:** difficulty in explaining decisions made by complex algorithms, particularly those based on neural networks [9].

• **Strategic risk:** loss of customer trust, potentially affecting long-term banking relationships and institutional reputation.

• **Link to IS governance:** ISO standards [4][16], while effective in clarifying governance responsibilities, remain too generic to address opacity and shared responsibility between humans and AI.

III.2.3 SYNTHESIS

These two cases demonstrate that the risks identified in the literature—algorithmic bias [14][6], insufficient explainability [9][10], and grey areas of responsibility [11][12]—are already materializing in practice. before need for more dynamic and ethical governance, capable of anticipating and correcting AI-related deviations before they produce large-scale negative effects. As shown by Floridi, Cowls, and Taddeo (2023) [17], European AI governance now emphasizes transparency, traceability, and algorithmic accountability, complementing traditional frameworks such as ISO and COBIT.

III.3 KEY FINDINGS

The combined analysis of the literature review and case studies reveals four major limitations of traditional frameworks when applied to AI systems:

III.3.1 ETHICS AND ACCOUNTABILITY

Established frameworks such as COBIT [2] and ISO 38500 [4] emphasize control, compliance, and strategic alignment, but they do not explicitly provide mechanisms to integrate principles of algorithmic ethics (fairness, non-discrimination, respect for human rights) [6][7][8]. This gap creates a normative vacuum: if an algorithm reproduces bias, there is no clear internal process to identify and correct it. The Amazon case [14] illustrates this limitation, as the absence of ethical tools embedded in governance led to the deployment of a discriminatory system, directly affecting the fairness of recruitment processes. As shown by Floridi, Cowls, and Taddeo (2023) [17], European AI governance now emphasizes transparency, traceability, and algorithmic accountability, complementing traditional frameworks such as ISO and COBIT.

III.3.2 EXPLAINABILITY AND AUDITABILITY

Frameworks such as ITIL [3] and ISO 38500 [4] define quality and auditability processes for IT services, but they are not designed to manage opaque AI models, particularly deep neural networks [9][10][15]. This makes it extremely difficult to explain algorithmic decisions to users or regulators. The Apple Card case [10][15][15] illustrates this challenge: despite structured IT governance, Apple was unable to provide clear explanations of its scoring model's logic, fueling distrust among customers and regulatory authorities.

III.3.3 RESPONSIBILITY AND LIABILITY

Current standards define general responsibilities (e.g., ISO 38500 [4]) but do not specify who should be held accountable when an AI-driven decision causes harm: the algorithm designer, the data team, IT management, or the organization as a whole [11][12]. This grey area weakens governance. In Apple's case, when customers challenged credit-scoring decisions, it was difficult to identify the true party responsible—the tool, the technical team, or senior management [10]. This legal and organizational uncertainty exposes companies to significant reputational and financial risks.

III.3.4 OVERLY SLOW EVOLUTION CYCLES

Recent trends identified by Gartner (2024) [18] confirm that organizational maturity in AI governance depends on the ability to automate compliance and integrate continuous feedback loops into management frameworks. ISO and ITIL frameworks rely on lengthy update and standardization processes, sometimes spanning several years [13][16]. By contrast, AI models evolve on much faster cycles, sometimes within months. This mismatch creates misalignment between the pace of technological innovation and the adaptability of governance mechanisms. In the Amazon case, the recruitment tool generated bias before corrective governance measures could be implemented. The slowness and rigidity of frameworks prevented a proactive response, exacerbating ethical and reputational consequences.

III.4 ANALYTICAL SYNTHESIS

These shortcomings show that traditional frameworks, while effective for managing conventional information systems, are insufficient to address the challenges specific to AI. Amazon illustrates the ethical and reputational risks associated with the absence of bias control, while Apple highlights issues of transparency, fairness, and accountability. Taken together, these cases underscore the need for more agile, explainable, and accountability-driven governance capable of keeping pace with rapid technological change and preventing societal harm.

XV. METHODOLOGY

Table 1: Strengths, Limitations, and Proposed Adaptations of Major Governance Frameworks in the Context of AI

Framework	Strengths	Limitations in the Face of AI	Proposed Adaptations
COBIT 2019 [11]	Strategic/IS alignment, value management	Does not address bias and ethics [5][15]	Merging IS/AI committees [18], ethical indicators
ITIL 4 [13]	Service management, continuous improvement	Cycles too slow, lack of explainability [1][7]	Extension toward MLOps [19], AI auditability
ISO/IEC 38500 [12]	Clarifies governance responsibilities	Too generic, insufficient for AI-related risks [10]	Integration of the AI Act [10], human/AI accountability
ISO/IEC 23053 [19]	Framework for managing AI systems	Insufficient ethical and organizational coverage [5]	AI Centers of Excellence [9], standardized audits
IEEE 2857/2863 [17][18]	AI governance, privacy	Limited adoption, weak IS integration	COBIT/ITIL harmonization, ethical KPIs

The table highlights that while traditional governance frameworks provide strong structural foundations, they require significant adaptation to address the ethical, technical, and organizational challenges introduced by artificial intelligence.

CRITICAL ANALYSIS

The comparative review highlights several key insights:

1. No comprehensive coverage of AI challenges
Each framework contributes a useful dimension (control with

COBIT, quality with ITIL, clarification of responsibilities with ISO 38500, technical management with ISO 23053, ethics and privacy with IEEE). However, none of them individually addresses the full range of AI-related issues: bias, explainability, accountability, and rapid innovation cycles.

2. An imbalance between technical and ethical approaches

ISO and ITIL frameworks primarily focus on organizational and technical aspects (quality, processes, service management), whereas emerging frameworks such as IEEE place greater emphasis on privacy and ethics. This imbalance creates a risk of fragmented practices if organizations fail to effectively articulate and integrate these approaches.

3. Slow adaptation to the rapid cycles of AI

Historical frameworks (COBIT, ITIL, ISO 38500) rely on lengthy update processes. Yet AI technologies evolve within months. This mismatch prevents governance mechanisms from keeping pace and increases the risk of harmful outcomes before corrective measures can be implemented.

4. Emerging initiatives still limited

IEEE standards and ISO/IEC 23053 represent a significant step toward AI-adapted governance, but their adoption remains embryonic. Their integration with traditional frameworks is still weak, hindering the development of a coherent and universal governance framework.

Conclusion of the Comparative Analysis

The World Economic Forum (2024) [20] also emphasizes that AI governance must be supported by global audit and transparency frameworks, while the European Data Protection Board (2025) [19] stresses the compatibility between data protection and algorithmic governance.

This study confirms that while each framework represents a piece of the puzzle, none provides a complete solution to the challenges posed by AI. This justifies the proposal of a hybrid governance model, combining the structural robustness of existing frameworks with new mechanisms (algorithmic ethics, explainability, agile cycles, and ethical performance indicators). Such a model should also promote normative interoperability between established standards (COBIT, ITIL, ISO) and emerging ones (IEEE, AI Act), in order to ensure more coherent and resilient governance. As shown by Floridi, Cowls, and Taddeo (2023) [17], European AI governance now emphasizes transparency, traceability, and algorithmic accountability, complementing traditional frameworks such as ISO and COBIT.

V. CONTRIBUTIONS

V.1 THEORETICAL CONTRIBUTION

This research proposes an extension of traditional governance frameworks to integrate the specificities of artificial intelligence. The approach is designed as a multi-level model (strategic, tactical, and operational), enabling coverage of global steering needs, organizational implementation, and the technical management of AI systems.

V.1.1 STRATEGIC LEVEL: TOWARD INTEGRATED AND RESPONSIBLE GOVERNANCE

At the highest level, this study recommends merging IS and AI governance committees. This integration makes it possible to move beyond a siloed view of technology and governance and to establish a holistic approach aligning:
• the organization's strategic objectives with AI use cases;
• value creation (innovation, competitiveness, efficiency) with societal responsibility (ethics, sustainability, inclusion) [16];
• proactive consideration of reputational and regulatory risks, particularly with the entry into force of the European AI Act.

This integrated governance addresses the need to ensure that AI is not merely an optimization tool, but also a vector of trust and legitimacy for internal and external stakeholders.

V.1.2 TACTICAL LEVEL: INSTITUTIONALIZING AI GOVERNANCE

At the organizational level, the study proposes the creation of an AI Center of Excellence within the IT department. Its mission is twofold:

1. **Standardization and compliance:** ensuring compliance with emerging regulations (AI Act [12], IEEE standards [16]) and recognized governance principles (ISO, COBIT).

2. **Development of internal capabilities:** training employees, raising awareness of algorithmic bias and ethical issues, and fostering an organizational culture of digital responsibility [9].

This center would act as a bridge between corporate strategy and operational teams, facilitating the adoption of consistent practices and avoiding fragmented approaches.

V.1.3 OPERATIONAL LEVEL: MANAGING THE AI MODEL LIFECYCLE

Finally, at the technical level, the study recommends adopting MLOps (Machine Learning Operations) practices. Inspired by DevOps methods, this model aims to:

• integrate AI model management into continuous development, deployment, and monitoring cycles [5];

• ensure traceability and auditability of models throughout their lifecycle (from training to production updates);

• enable greater responsiveness to the rapid evolution of algorithms and regulatory contexts.

The integration of MLOps directly addresses the limitations of traditional frameworks, particularly their slow adaptability and lack of continuous model monitoring.

V.2 INTEGRATIVE AND EVOLUTIONARY CONTRIBUTION

The added value of this contribution lies in its ability to articulate three complementary levels of governance, thereby combining:
• strategic vision (alignment, responsibility, legitimacy);
• tactical organization (structures, skills, compliance);
• operational efficiency (dynamic and ethical management of AI models).

This multi-level model provides an evolutionary framework capable of strengthening the robustness and legitimacy of governance systems while integrating the disruptive specificities of AI.

VI. LIMITATIONS AND FUTURE RESEARCH

VI.1 LIMITATIONS

• **Sectoral scope:** the study covers technology, banking, and logistics, but not healthcare or public administration, where issues such as confidentiality and social equity are critical [7].

• **Regulatory maturity:** the European AI Act [12] is still being deployed, making it difficult to assess its real impact.

• **Limited adoption of emerging standards:** IEEE 2857/2863 [15][16] are not yet widely adopted.
• **Speed of evolution:** governance frameworks risk becoming obsolete if AI continues to evolve faster than normative processes [13].

VI.2 FUTURE DIRECTIONS

• Extend the analysis to critical sectors (healthcare, education, strategic industries, public administrations).

• Explore the coexistence of AI with other disruptive technologies (quantum computing, blockchain).

• Develop ethical performance indicators integrated into existing frameworks.

• Empirically test the effectiveness of hybrid approaches through pilot projects.

• Promote normative interoperability between traditional frameworks and emerging standards [15][16][16].

VII. CONCLUSION

The World Economic Forum (2024) [20] also emphasizes that AI governance must be supported by global audit and transparency frameworks, while the European Data Protection Board (2025) [19] stresses the compatibility between data protection and algorithmic governance.

Information systems governance is at a strategic turning point in the face of the massive rise of artificial intelligence. Traditional frameworks such as COBIT, ITIL, and ISO [2][4][3], while providing a solid foundation, do not fully address AI-specific challenges, particularly ethics, transparency, and rapid evolution [6][10][12]. As shown by Floridi, Cowls, and Taddeo (2023) [17], European AI governance now emphasizes transparency, traceability, and algorithmic accountability, complementing traditional frameworks such as ISO and COBIT.

This study demonstrates that only a hybrid, multi-level approach can meet these challenges. At the strategic level, merging IS and AI committees aligns performance, innovation, and societal responsibility. At the tactical level, establishing an AI Center of Excellence within the IT department ensures regulatory compliance and skills development [9][12][15]. At the operational level, adopting MLOps practices guarantees comprehensive and transparent management of the AI model lifecycle [16].

This model not only provides a framework for steering and control but also transforms AI into a lever for sustainable value creation and societal trust. By combining rigor, agility, and ethical integration, IS governance can anticipate and mitigate risks while maximizing innovation.

Future evolution must remain dynamic and sector-specific, capable of adapting to new regulations, emerging technical standards, and disruptive technologies. This transformation paves the way for responsible, high-performing, and sustainable governance, in which AI becomes a reliable and ethical driver of innovation. The World Economic Forum (2024) [20] also emphasizes that AI governance must be supported by global audit and transparency frameworks, while the European Data Protection Board (2025) [19] stresses the compatibility between data protection and algorithmic governance.

REFERENCES

[1] McKinsey Global Institute, *The State of AI in 2023: Generative AI's Breakout Year*, McKinsey & Company, 2023.

[2] ISACA, *COBIT 2019 Framework: Introduction and Methodology*, ISACA Press, 2019.

[3] AXELOS, *ITIL Foundation Essentials – ITIL 4 Edition*, TSO, 2019.

[4] ISO/IEC, *ISO/IEC 38500:2024 – Information Technology: Governance of IT for the Organization*, International Organization for Standardization, 2024.

IJOA.

[5] ISO/IEC JTC 1/SC 42, *ISO/IEC 23053:2023 – Framework for AI Systems Using Machine Learning*, International Organization for Standardization, 2023.

[6] A. Jobin, M. Ienca, E. Vayena, *The Global Landscape of AI Ethics Guidelines*, Nature Machine Intelligence, vol. 1, no. 9, pp. 389–399, 2019.

[7] Organisation de Coopération et de Développement Économiques (OCDE), *Recommendation of the Council on Artificial Intelligence*, OECD Publishing, 2019.

[8] UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, UNESCO Publishing, 2021.

[9] S. Amershi, D. Weld, M. Vorvoreanu, A. Fourney, B. Nushi, P. Collisson, et al., *Guidelines for Human–AI Interaction*, Proceedings of the CHI Conference on Human Factors in Computing Systems, pp. 1–13, 2019.

[10] I.D. Raji, A. Smart, R.N. White, M. Mitchell, T. Gebru, B. Hutchinson, et al., *Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing*, Proceedings of the ACM Conference on Fairness, Accountability, and Transparency (FAccT), pp. 33–44, 2020.

[11] S. Russell, *Human Compatible: Artificial Intelligence and the Problem of Control*, Viking Press, 2019.

[12] Commission Européenne, *Regulation (EU) 2024/1689 on Artificial Intelligence (AI Act)*, Official Journal of the European Union, 2024.

[13] E. Brynjolfsson, A. McAfee, *The Business of Artificial Intelligence*, Harvard Business Review, vol. 95, no. 4, pp. 3–11, 2017.

[14] S. Barocas, M. Hardt, A. Narayanan, *Fairness and Machine Learning*, fairmlbook.org, 2019.

[15] New York State Department of Financial Services, *Report on the Apple Card Investigation*, NYDFS Publications, 2021.

[16] IEEE Standards Association, *IEEE 2863-2022 – Recommended Practice for Organizational Governance of Artificial Intelligence*, IEEE Press, 2022.

[17] L. Floridi, J. Cowls, M. Taddeo, *The Ethics of Artificial Intelligence: A European Perspective on Trustworthy AI Governance*, AI & Society, 2023.

[18] Gartner, *AI Governance Trends and Best Practices for 2024*, Gartner Research, 2024.

[19] European Data Protection Board, *Guidelines on AI Systems and Data Protection*, EDPB Publications, 2025.

[20] World Economic Forum, *AI Governance and Accountability Framework: Building Trust in AI*, World Economic Forum Publications, Geneva, 2024