

Building a Minimal Governance Framework for Automated Decisions: A Practical Approach for Early-Stage Organizational Adoption

Cristina-Mihaela STANCIU*

National University of Science and Technology POLITEHNICA Bucharest, Bucharest, Romania

**Corresponding author, cristina.stanciu00@upb.ro*

Augustin SEMENESCU

National University of Science and Technology POLITEHNICA Bucharest, Bucharest, Romania

Academy of Romanian Scientists, Bucharest, Romania

augustin.semenescu@upb.ro

Abstract. *This article aims to explore the way in which a minimal framework of governance might be designed for organizations that start adopting systems based on artificial intelligence (AI). The article focuses on the operational principles which managers could introduce even in early stages, like functional transparency, a clear allocation of responsibilities, preliminary checks regarding algorithmic risks and a basic approval flow which must ensure the oversight of the decision-making process. These measures could support operational control on a daily basis and could help organizations to follow GDPR requirements without the implementation of complex systems. The analysis reflects the realities faced by small and medium-sized entities (SME), where limited technical expertise, lack of internal policies regarding intelligent technologies and the dependency of external suppliers influence implementation choices. This article underlines that a simplified managerial architecture with educational and oversight roles, may facilitate the transition to the automated decision-making process. This offers a practical starting point that organizations can later expand into governance mechanisms.*

Keywords: managerial governance, early-stage AI adoption, organizational control, automated decisions, algorithmic risk, transparency, GDPR alignment, operational oversight, SME challenges, AI governance frameworks.

Introduction

The adoption of AI-based decision making systems has become a frequent practice in today's organizations, including these that are in an early stage of digital development. The greater availability of standardized commercial solutions allows organizations to integrate algorithmic tools in operational processes with relatively low entry barriers. As a result, the automated decision-making process might be implemented even in contexts where advanced governance structures or internal and consolidated technical expertise are lacking. (OECD, 2023a; Peretz-Andersson et al., 2024). In many cases, these systems are introduced through standard software solutions or external services providers, reducing the need for internal development and accelerating the implementation.

In this operational context, automated decisions are used for activities such as classification, preliminary evaluation, filtering or prioritization. These functions frequently support managerial activities by processing a large data volume and generating standardized results that support future actions. Over time, these types of systems tend to integrate into current organizational practices, influencing decision-making flows and modelling internal processes, even though their role is

initially perceived as being auxiliary. This gradual integration increases the practical relevance of automated decision-making process for organizational control and the assumption of responsibility.

The extensive use of AI takes place in a normative environment which establish explicit obligations regarding data protection and decision-making responsibility. The General Data Protection Regulation is applicable no matter the organization's size or level of maturity and its provisions regarding to transparency, rights to human intervention and protection of individuals apply both to large-scale and limited implementation. (EDPB, 2023; Thouvenin, 2024). . In consequence, early-stage organization adopting digital technologies are not exempt from legal obligations of compliance, even though automated systems are experimentally implemented or on a small scale.

Recent literature highlights persistent difficulties in transposing these normative requirements in operational practices within the framework of early stage organizations. A recurrent challenge regards the lack of internal mechanisms capable pf monitoring, documenting and evaluating automated decisions in a systematic manner. Limited resources, fragmented responsibilities and lack of formalized processes restrict these organizations' capacity to assure continuous compliance within data protection requirements. (OECD, 2023b). These constrains increase the risk of decalage emerging between legal requirements and daily decision-making practices.

In this context, the main issue addressed by the present article is the lack of governance frameworks adapted to early-stage organizations adopting automated process. Existing models of governance are designed for a large scale for mature organizations, which have dedicated departments for compliance, specialized human resources and stable organizational structures. As a result, their implementation in small or medium-sized entities or in organization at an early stage of development is often impracticable or disproportionate in relation to available capacities. (Batoool et al., 2023; Peretz-Andersson et al., 2024). This situation generates an operational gap between legal requirements and real organizational practices, leaving early adopters without workable guidance.

This situation creates an operational gap between regulatory expectations and actual organizational practices, particularly in early-stage contexts (see Figure 1).

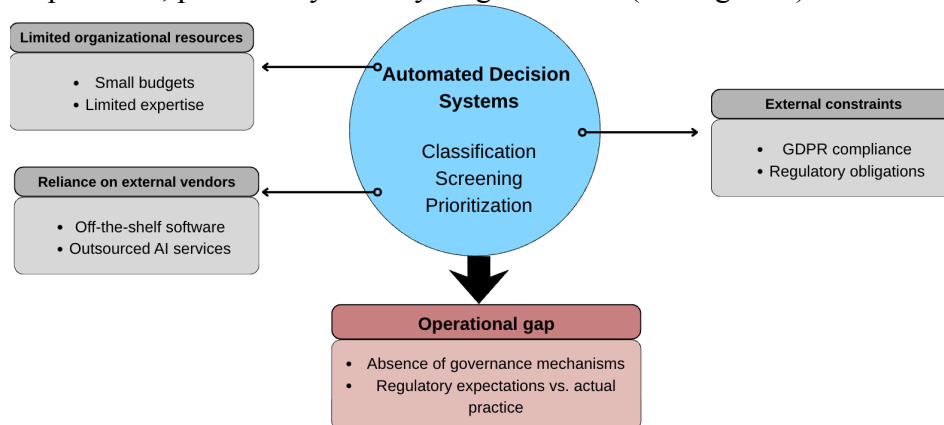


Figure 1. Positioning of automated decisions in early-stage organizations

Author's own elaboration.

This article adopts a conceptual-applied approach focused on the design of a minimal governance framework designed to support a based managerial control on automated decisions.

The proposed approach is designed from a managerial perspective and follows the implementation of the functional requirements of the GDPR without transforming the governance into a predominantly legal exercise. On the other hand, the governance is treated as an element of managerial oversight, focusing on role clarity, decisions' traceability and fundamental mechanisms regarding the assumption of responsibilities which can be maintained even when there are limited resources. (Ligot, 2024; EDPB, 2023).

The research question that guides this study is the following: how can a minimal governance framework be designed which allows early-stage organization to maintain managerial control and a basic level of compliance with GDPR requirements when complex organizational structures are lacking? The main hypothesis is that a set of simple and operational principles might support decision-making control and might facilitate gradual development of governance mechanisms in time. It is considered that such principles functions as transitional mechanisms, allowing organizations to incrementally adapt their governance practices when the use of automated decision-making processes expands. (Batool et al., 2023).

Literature review

State of the art on automated decision-making and AI governance

Academic literature published after 2023 increasingly treats the automated decision-making process as a core component of today's organizational transformation with direct implications on managerial control, the assumption of responsibilities and risks distribution. Automated decisions are no longer analyzed as technical results of algorithmic systems, but as organizational practices which reconfigure the way in which the authority, responsibility and oversight are exercised. Within this research direction, AI governance is frequently defined as a set of institutional, organizational, and operational mechanisms designed to ensure the controlled and responsible use of algorithmic systems throughout their life cycle, from design and implementation to monitoring and reviewing. (Floridi & Taddeo, 2024).

Recent studies underline that AI governance models follow a set of principles such as traceability, responsibility and reducing risks, especially in decision-making contexts which affects individuals' rights or produce relevant legal effect. The traceability is discussed as being the capacity to reconstruct the way in which a decision was generated, including the use of data sources, model's logic and involved organizational actors. Responsibility is presented as the possibility to assign responsibility for decisions generated or supported by automated systems, even in situations where direct human intervention is limited. Risk reduction focuses on the identification and diminution of potential harms associated to automated decisions, including discrimination, error propagation and lack of explanation. (Batool et al., 2023).

From the information systems perspective, the literature highlights the fact that introducing AI into decision-making processes modifies the main logic of organizational control. Traditional managerial control mechanisms based on direct oversight are replaced or complemented by different forms of at systems-level oversight. The managers must evaluate algorithmic systems' performance through indicators, thresholds, exception reports, and feedback loops, rather than reviewing individual decisions ex post. (Shrestha et al., 2023). This change reflects a structural reconfiguration of management functions as a response to algorithmically mediated decision-making environments.

The authors describe this transformation as an adaptation of managerial control to decision-making processes characterized by scale, speed and partial opacity. Once decisions are generated in large volume and often in real time, traditional forms of review process become unpredictable. In

consequence, governance mechanisms are reorientated toward monitoring systems behaviors, evaluating results distribution and identifying discrepancies. This evolution raises questions regarding the adaptability of existing control frameworks and the extent to which” these can be applied in different organizational contexts.

Managerial control and organizational risk in automated decisions

Recent literature in the field of management suggests that the risks associated with decision making process are multidimensional. These risks include technical risk such as model errors or data quality, issues operational risk associated to process integration and system dependency, legal risk generated by non-compliance with legal requirements regarding data protection or discrimination, but also reputational risk linked to public scrutiny and the trust of stakeholders. In an important way, these risks are not treated as simple isolated technical deviations but as results of interaction between algorithmic systems and existing organizational structures. (Batoool et al., 2023).

Empirical studies highlight that algorithmic systems may introduce systematic errors or biases which quickly propagate in the decision-making process framework even when they are implemented in limited or pilot context. Due to the scalability of automation small inaccuracies but the model level may lead to repeated effects or amplified in multiple decisions. This amplification effect is highly relevant in situation where the automated results are used as implicit inputs for future managerial actions. Reducing in this way the possibility to corrective intervention.

From a managerial perspective, the literature underlines that traditional control mechanisms are often insufficient for managing these risks. Automated decision-making processes reduce the direct visibility. Into the way individual decisions are generated and complicate the assumption of responsibilities, especially organizations with limited resources or fragmented roles. (Štrukelj & Dankova, 2025). Responsibility may be dispersed between software suppliers’ data sources system operator managers generating ambiguities in accountability structures.

In response recent research highlights the need for adequate mechanisms for managerial control to system-orientated oversight. Instead of focusing on individual decisions the managers are encouraged to oversight the conditions in which the decisions are generated including data governance practices models, updating procedures and escalation processes for abnormal results. (Shrestha et al., 2023). This approach defines control as a continuous managerial function integrated in organizational processes and not as a corrective activity performed later.

Adoption of AI in early-stage organizations and SMEs

A substantial segment of recent literature examines the adoption of artificial intelligence in organizations at early stages of digitalization, with particular attention to small and medium-sized enterprises. These studies consistently indicate that early-stage organizations adopt AI in an incremental and pragmatic manner, driven primarily by short-term operational efficiency rather than by comprehensive digital transformation strategies (Peretz-Andersson et al., 2024).

Implementation frequently occurs through standardized commercial solutions provided by external vendors. This approach reduces initial investment and technical complexity but also limits organizational control over model design, data processing logic, and system updates. As a result, decision-making capabilities are partially outsourced, and internal understanding of how decisions are generated remains limited.

The literature highlights that reliance on external providers can increase organizational and legal risks, particularly in the absence of internal policies governing AI use. Limited technical expertise and the lack of formal governance structures lead early-stage organizations to deploy

automated systems without adequate mechanisms for evaluation, documentation, or oversight (Peretz-Andersson et al., 2024; Štrukelj & Dankova, 2025). These conditions increase vulnerability to compliance failures and reduce the organization's capacity to respond effectively to errors or complaints.

Researchers argue that these constraints justify the development of governance frameworks adapted to low levels of organizational maturity. Rather than replicating models designed for large or technologically advanced organizations, governance mechanisms for early-stage adopters should reflect resource limitations, simplified structures, and evolving capabilities.

Algorithmic auditing and lightweight control mechanisms

Algorithmic auditing is discussed in recent literature as a central instrument for ensuring accountability and reducing risks associated with automated decisions. Classical audit models, however, are widely described as difficult to implement in organizations with limited resources, due to their technical complexity, documentation requirements, and associated costs.

These approaches are based on simple checks, periodical reviews and targeted evaluation which may be performed without specialized technical teams. The focus is on early identification of highlighted risks linked by data quality, the purpose of the decision and the potential impact individuals.

Such mechanisms are designed to be integrated into existing managerial routines rather than introduced as separate compliance structures. Literature suggests that lightweight auditing can support basic managerial control during early phases of AI adoption by enabling organizations to identify problematic patterns, document key assumptions, and establish minimal escalation procedures (Hacohen, 2023). This approach prioritizes feasibility and continuity over exhaustive technical validation.

Legal perspective on automated decisions and GDPR requirements

Legal scholarship published after 2023 focuses extensively on the interpretation and application of Article 22 of the GDPR and the obligations arising from decisions based solely on automated processing. Studies emphasize that rights related to transparency, human intervention, and contestation should be interpreted functionally and embedded within organizational processes, rather than addressed through formal compliance statements alone (Thouvenin, 2024).

Purely formal approaches to compliance are widely regarded as insufficient for ensuring effective protection of data subject rights. Instead, legal requirements are increasingly linked to organizational practices, such as documenting decision logic, defining intervention points, and assigning responsibility for responding to challenges.

In early-stage organizations, the literature identifies significant difficulties in implementing GDPR requirements due to the absence of dedicated compliance structures. Recent research supports proportional approaches that enable basic alignment with legal obligations through simple, managerially driven mechanisms (EDPB, 2023). This perspective reinforces the integration of legal governance into minimal managerial architectures rather than treating it as a separate legal function.

As illustrated in Figure 2, the convergence of these literature streams reveals the absence of governance frameworks adapted to early-stage organizations.

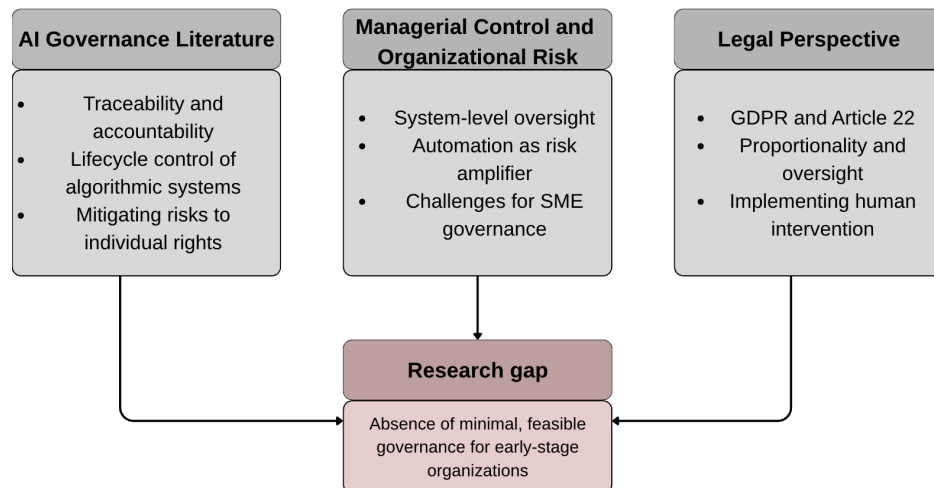


Figure 2. Synthesis of literature streams and the research gap

Author's own elaboration

Research gap and positioning of the study

Although existing literature provides extensive analyses of AI governance, managerial control, and legal requirements related to automated decisions, these dimensions are predominantly examined within models designed for mature organizations. There is a lack of conceptual frameworks that explicitly describe a minimal level of governance adapted to the constraints faced by organizations in early stages of AI adoption (Batoool et al., 2023; Floridi & Taddeo, 2024).

This study positions itself within this gap by proposing a minimal governance framework conceived as a transitional solution. The contribution lies in articulating a set of operational principles that can be implemented rapidly to support managerial control and basic alignment with GDPR requirements, without imposing complex organizational structures. The proposed framework is intended to function as an initial layer of governance that can evolve alongside organizational maturity and expanded use of automated decision-making systems.

Methodology

The research employs a conceptual–applied design grounded in a thematic analysis of academic literature published after 2023 that addresses AI governance, managerial control, and automated decision-making. The methodological approach is qualitative and is oriented toward synthesizing existing theoretical and applied contributions in order to identify patterns, convergences, and gaps relevant to early-stage organizational contexts. Rather than seeking empirical generalization, the analysis focuses on extracting operational insights that can inform governance design under conditions of limited organizational resources.

The thematic analysis examines how recent literature conceptualizes governance mechanisms, responsibility structures, and control practices in relation to automated decisions. Particular attention is given to contributions that discuss the practical implementation of governance principles, as opposed to purely normative or abstract models. This approach allows for the identification of operational principles that can be realistically adopted by organizations with constrained technical expertise, limited staffing, and evolving digital practices.

Source selection was guided by two main criteria: relevance to early-stage organizational contexts and the academic rigor of the publications. Priority was given to peer-reviewed journal articles, policy-oriented academic reports, and authoritative contributions that explicitly address small and medium-sized enterprises or organizations in initial phases of AI adoption. This selection

strategy ensures that the analysis reflects both theoretical developments and applied perspectives that are applicable beyond highly mature or resource-intensive organizational settings.

The underlying methodological assumption is that organizational feasibility constitutes the central criterion for designing a minimal governance framework. Feasibility is understood in terms of proportionality between governance requirements and organizational capacity, including managerial time, expertise, and formal structures. On this basis, the research treats feasibility not as a secondary constraint, but as a defining principle that shapes which governance mechanisms can be meaningfully implemented at early stages of automated decision-making adoption.

Results and discussions

The proposed minimal governance framework is conceived as a foundational operational architecture intended for organizations in the early stages of adopting automated decision-making systems. It is designed to respond to the structural and resource constraints that typically characterize early-stage organizations and small and medium-sized enterprises. The framework rests on the premise that artificial intelligence governance does not need to be fully institutionalized at the outset in order to be effective. Instead, governance can be configured as a gradual and adaptive process, aligned with organizational maturity, scale of AI use, and available managerial capacity, without presupposing advanced control structures or specialized governance units (Batoool et al., 2023; Ligot, 2024). The proposed minimal governance framework is summarized in Figure 3 and is detailed below.

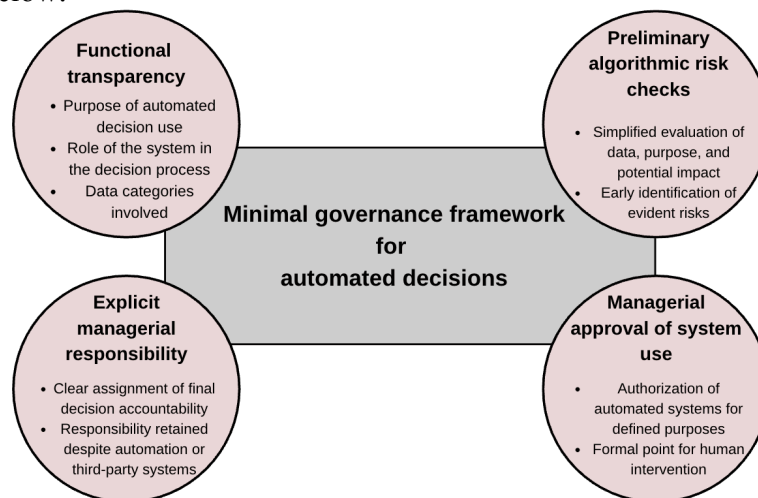


Figure 3. Minimal governance framework for automated decisions

Author's own elaboration.

This assumption reflects a growing recognition in the literature that governance requirements must be interpreted proportionally. Early-stage organizations often lack the financial, technical, and human resources necessary to implement comprehensive governance models developed for mature enterprises. As a result, the absence of advanced structures does not imply the absence of governance, but rather the need for governance mechanisms that are simplified, operational, and embedded in existing managerial routines. The proposed framework responds to this need by identifying a limited set of core principles that can sustain basic oversight and accountability during the initial phases of automated decision-making adoption.

The framework is structured around the idea that managerial control over automated decisions can be exercised through a small number of clearly defined and practically

implementable mechanisms. These mechanisms are not intended to substitute advanced governance models but to function as a baseline that enables organizations to maintain oversight, allocate responsibility, and manage evident risks. The framework is therefore conceptualized as a transitional arrangement that supports immediate managerial needs while remaining open to future expansion and refinement as organizational capabilities evolve.

The first pillar of the framework is functional transparency. Functional transparency is defined as the organization's capacity to clearly articulate the purpose of using automated systems, the categories of data involved, and the role these systems play within broader decision-making processes. This form of transparency focuses on managerial and organizational understanding rather than on full technical explainability of algorithmic models. The literature consistently notes that detailed model-level explanations are often inaccessible in standardized commercial solutions, particularly when systems are procured from external vendors (Thouvenin, 2024; EDPB, 2023).

From a managerial perspective, functional transparency supports informed oversight by enabling decision-makers to understand what automated systems are used for, what inputs they rely on, and how their outputs influence organizational actions. This understanding is essential for evaluating whether the use of automation aligns with organizational objectives and regulatory constraints. Functional transparency also facilitates communication with internal stakeholders and external actors, including regulators and affected individuals, by providing clear and consistent descriptions of system use.

The second pillar of the framework concerns the clear delineation of managerial responsibilities. In automated decision-making environments, responsibility can easily become fragmented or ambiguous, particularly when systems are developed, maintained, or operated by third-party providers. The absence of explicit responsibility allocation increases the risk of accountability gaps, where no single role assumes ownership of decision outcomes. The proposed framework addresses this issue by recommending the explicit assignment of final decision responsibility to a defined managerial role, regardless of the level of automation involved (Štrukelj & Dankova, 2025).

This allocation of responsibility reinforces the principle that automation does not eliminate managerial accountability but transforms how it is exercised. Even when decisions are generated or supported by algorithmic systems, a designated manager remains responsible for authorizing system use, responding to identified risks, and addressing potential challenges or complaints. Clear responsibility allocation also supports internal escalation procedures and clarifies decision ownership in interactions with external stakeholders.

The third pillar consists of preliminary assessments of algorithmic risks. These assessments take the form of simplified evaluations focused on three core elements: the data used by the system, the intended purpose of its deployment, and the potential impact of its outputs. Unlike comprehensive technical audits, these assessments are designed to be feasible with limited expertise and resources. They aim to identify evident risks, such as inappropriate data sources, misalignment between system outputs and organizational objectives, or potential negative effects on individuals.

Recent literature refers to such mechanisms as "lightweight audits," emphasizing their role as early-stage risk detection tools rather than exhaustive validation instruments (Hacohen, 2023). Within the proposed framework, preliminary risk checks function as a structured managerial exercise that encourages reflection on system use before and during deployment. By incorporating these evaluations into routine managerial decision-making, organizations can reduce exposure to avoidable risks without introducing complex or costly procedures.

The fourth pillar involves the establishment of a simple managerial approval flow governing the use of algorithmic systems. This approval process requires that automated systems are explicitly authorized for specific purposes prior to deployment. The approval flow is intended to ensure that system use is deliberate, documented, and aligned with organizational objectives. It also provides a formal point of human intervention, supporting GDPR requirements related to decision oversight and responsibility (EDPB, 2023; Shrestha et al., 2023).

From an operational standpoint, a basic approval flow contributes to consistency and traceability. It creates a record of managerial intent and clarifies the scope within which automated decisions are permitted. This mechanism also facilitates periodic review, as approved uses can be reassessed in light of changes in organizational needs, regulatory interpretations, or system performance.

The framework is explicitly designed as a transitional instrument rather than a fixed governance model. As organizations gain experience with automated decision-making and expand their use of artificial intelligence, additional governance layers can be introduced incrementally. These may include more formal documentation practices, enhanced monitoring mechanisms, or more detailed audit procedures. The gradual expansion of governance arrangements allows organizations to align governance complexity with organizational maturity and risk exposure (Peretz-Andersson et al., 2024).

Conceptual results derived from the framework indicate that meaningful governance of automated decisions can be exercised even in the absence of advanced institutional structures. The analysis suggests that minimal mechanisms, when coherently combined, can support managerial control and decision accountability in early-stage contexts (Batool et al., 2023). This finding challenges the assumption that effective AI governance necessarily requires comprehensive or resource-intensive arrangements.

From a managerial perspective, the framework supports a reconfiguration of organizational control by shifting attention away from individual automated decisions toward the conditions under which algorithmic systems are used. Control is exercised through oversight of purposes, data inputs, responsibility allocation, and approval processes, rather than through direct evaluation of each decision outcome (Shrestha et al., 2023). This system-oriented approach reduces implementation costs and lowers barriers to adoption, making it suitable for organizations with limited resources.

From a legal perspective, the functional integration of GDPR requirements into managerial processes helps reduce the gap between formal compliance and actual control. By embedding transparency, responsibility, and human intervention mechanisms into everyday managerial practices, the framework facilitates decision traceability and supports the exercise of data subject rights (EDPB, 2023; Thouvenin, 2024). This approach enables proportional compliance strategies that are compatible with early-stage organizational realities.

At the same time, the framework has clear limitations in high-risk contexts, such as those involving significant legal, social, or economic consequences. In such situations, minimal governance mechanisms are insufficient on their own and must be complemented by more robust audit, evaluation, and oversight processes. The literature consistently emphasizes that minimal governance should be understood as an initial stage within an evolving governance trajectory, rather than as a comprehensive solution applicable to all contexts (Ligot, 2024).

Conclusion

The research demonstrates that the governance of automated decision-making can be conceptualized as a gradual process that is adaptable to different levels of organizational maturity. Rather than treating AI governance as a fixed or binary condition, the findings support an evolutionary understanding in which governance arrangements develop alongside organizational capabilities, resources, and experience with automated systems. Within this perspective, governance is not dependent on the immediate availability of advanced institutional structures, but can be initiated through proportionate and operational mechanisms appropriate to early-stage contexts.

The proposed minimal framework enables early-stage organizations to exercise managerial control over automated decisions while ensuring basic alignment with GDPR requirements. By focusing on functional transparency, responsibility allocation, preliminary risk assessment, and managerial approval processes, the framework provides a structured yet feasible approach to oversight in environments characterized by limited resources and evolving digital practices. This confirms that meaningful control and accountability can be established even in the absence of comprehensive governance infrastructures (Batoool et al., 2023).

The primary contribution of the study lies in the conceptual delimitation of minimal governance and in the translation of abstract governance principles into mechanisms that can be applied immediately in organizational practice. Existing literature often addresses AI governance at a high level of abstraction or within models designed for technologically mature organizations. In contrast, this research operationalizes governance principles in a manner that is accessible to organizations at early stages of AI adoption, thereby reducing the gap between theoretical models and managerial application.

The relevance of the study also derives from extending the scope of AI governance research to organizational contexts that remain insufficiently addressed in existing scholarship. Early-stage organizations and small and medium-sized enterprises are increasingly exposed to automated decision-making through standardized commercial solutions, yet they are rarely the primary focus of governance frameworks proposed in the literature. By explicitly addressing these contexts, the research contributes to a more inclusive understanding of AI governance and responds to practical challenges identified in recent studies (Peretz-Andersson et al., 2024).

From a practical standpoint, the framework can be used as a transitional instrument and as a tool for managerial learning. It provides a structured basis for developing awareness of governance responsibilities and for embedding basic oversight practices into everyday managerial routines. In this sense, the framework supports not only compliance objectives but also organizational learning related to the responsible use of automated decision-making systems.

Future research directions include the empirical testing of the proposed framework across different organizational settings and sectors. Such studies would allow for the evaluation of its applicability, effectiveness, and limitations in practice. Further research may also explore the integration of the framework with emerging regulatory requirements, including those introduced by the AI Act, and assess how minimal governance arrangements can evolve in response to changing legal and technological conditions.

The limitations of the research are primarily related to its conceptual nature and the absence of empirical validation. The framework has not yet been tested in diverse organizational environments, and its effectiveness may vary depending on factors such as organizational size, sector, and risk exposure. These limitations underline the need for future empirical studies that

examine how minimal governance mechanisms function in practice and how they interact with more advanced governance structures as organizational maturity increases.

Acknowledgments: During the preparation of this work, the authors used ChatGPT-4 for language revision, translation support, and readability improvement. The use of AI-assisted translation and editing tools may influence the results of automated AI-content detection systems and could generate false-positive indications of AI-generated text. Following the use of these tools, the authors carefully reviewed, revised, and validated the final manuscript and assume full responsibility for the content of the publication.

References

- Batool, A., Arif, F., & Ghulam, S. (2023). Responsible artificial intelligence governance: A systematic literature review. *AI and Ethics*, 3(4), 1069–1089. <https://doi.org/10.48550/arXiv.2401.10896>
- EDPB. (2023). *Guidelines 05/2022 on the use of automated decision-making and profiling under Regulation (EU) 2016/679*. European Data Protection Board. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_en
- Floridi, L., & Taddeo, M. (2024). What is AI governance? *AI & Society*, 39(1), 1–14. <https://doi.org/10.1007/s00146-023-01635-y>
- Hacohen, U. Y. (2023). User-based algorithmic auditing. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4540163>
- Ligot, D. V. (2024). AI governance: A framework for responsible AI development. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4817726>
- OECD. (2023a). *Generative AI and the SME workforce*. OECD Publishing. https://www.oecd.org/en/publications/generative-ai-and-the-sme-workforce_2d08b99d-en.html
- OECD. (2023b). *Artificial intelligence and small and medium-sized enterprises*. OECD Publishing. <https://www.oecd.org/digital/artificial-intelligence-and-smes.htm>
- Peretz-Andersson, E., Tabares, S., Mikalef, P., & Parida, V. (2024). Artificial intelligence implementation in manufacturing SMEs: A resource orchestration approach. *International Journal of Information Management*, 77, 102781. <https://doi.org/10.1016/j.ijinfomgt.2024.102781>
- Shrestha, Y. R., Ben-Menahem, S. M., & von Krogh, G. (2023). Organizational decision-making with artificial intelligence. *Journal of Management Information Systems*, 40(1), 224–259. <https://doi.org/10.1177/0008125619862257>
- Štrukelj, T., & Dankova, P. (2025). Ethical leadership and management of small and medium-sized enterprises: The role of artificial intelligence in decision making. *Administrative Sciences*, 15(7), 274. <https://doi.org/10.3390/admsci15070274>
- Thouvenin, F. (2024). Article 22 GDPR on automated individual decision-making: A functional interpretation. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.5282535>