Available on: https://jefrr.ep-journals.org/ E-ISSN: 3051-3650, P-ISSN: 3051-3642

Journal of Economic Finance Research and Review

Volume: 02 Issue: 11 November 2026

Responsible AI Governance in Small and Medium-Sized Enterprises: Addressing Gaps in Data Governance, Algorithmic Transparency, And Accountability

Ly Bich Ngoc

Faculty of Economics, Hanoi Industrial and Trade University

Published Date: November 26, 2026 **Article DOI: 10.65150/EP-jefrr/V2E11/2026-18**

ABSTRACT: Artificial intelligence (AI) creates opportunities for small and medium-sized enterprises (SMEs) to improve productivity and decision-making, yet access to AI tools does not necessarily imply sufficient organizational capacity to govern associated risks. This study examines three governance gaps—data governance, transparency and explainability, and accountability—and proposes a responsible AI governance framework tailored to SMEs. A focused literature review is combined with conceptual analysis and comparison of international standards and relevant Vietnamese and European legal instruments. The analysis shows that SMEs face distinctive constraints arising from limited resources, multifunctional staff, fragmented data, and dependence on external AI providers. The proposed framework comprises six complementary components: direction and commitment; data governance; transparency and explainability; accountability and human oversight; risk and compliance; and capability and continuous improvement. The framework follows a proportional, risk-based logic rather than requiring SMEs to replicate governance systems designed for large organizations. Its practical value lies in translating broad responsible-AI principles into minimum controls that can be documented, monitored, and progressively strengthened. The study provides a conceptual basis for SMEs and supporting institutions to organize responsible AI governance while recognizing that the proposed framework and indicators require empirical validation.

KEYWORDS: responsible artificial intelligence, small and medium-sized enterprises, data governance, algorithmic transparency, explainability, accountability.

1. INTRODUCTION

AI is increasingly used for demand forecasting, business analytics, customer service, marketing, recruitment, and decision support. For SMEs, ready-made AI tools can reduce development costs and shorten implementation time. Nevertheless, OECD evidence indicates that AI adoption among SMEs remains below that of larger firms and that strategic and secure integration is uneven; skills, data, cost, and digital capacity remain important barriers [1], [2]. The resulting challenge is not simply technological adoption but the ability to maintain organizational control over systems whose outputs may affect customers, employees, partners, and business decisions.

This characteristic creates a significant governance problem: firms may deploy AI faster than they can establish effective controls. When external platforms are used, SMEs generally have limited direct control over the underlying model, training data, or update cycle. They nevertheless remain responsible for the purpose of use, the data supplied to the system, the verification of outputs, and decisions made within their operations. OECD, UNESCO, NIST, and ISO/IEC frameworks converge on transparency, accountability, risk management, human oversight, and continuous improvement as core elements of responsible AI governance [3]–[6].

The research gap is therefore not the absence of AI governance principles, but the difficulty of translating those principles into mechanisms that SMEs can actually implement. Studies on data quality [10], dataset documentation [11], algorithmic accountability [12], and model documentation [13] provide important building blocks, but they do not directly resolve how these elements should be integrated under conditions of limited resources, multifunctional roles, and dependence on external providers. This study addresses that gap by examining three interconnected governance areas—data governance, transparency and explainability, and accountability—and by proposing a proportional governance framework for SMEs.

The theoretical foundation combines stakeholder theory, which defines responsibility toward affected groups [7], institutional theory, which explains the influence of laws, standards, and market pressures [8], and the dynamic capabilities perspective, which treats AI governance as an organizational capability that must evolve with technology [9]. This combination positions responsible AI governance not merely as a compliance requirement but as an organizational mechanism for maintaining control in changing technological environments.

2. RESEARCH CONTENT

2.1. Research method

The study employs a focused literature review combined with conceptual analysis and comparison of governance standards. Sources include academic studies on data quality, transparency, and algorithmic accountability; official frameworks issued by OECD, UNESCO, NIST, and

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

ISO/IEC; and relevant legal instruments in Vietnam and the European Union. To define the SME context in Vietnam, the study also considers the Law on Support for Small- and Medium-Sized Enterprises and Decree No. 80/2021/ND-CP [19], [20].

The selection emphasizes sources that directly address data governance, explainability, accountability, risk management, organizational responsibility, and AI management systems. The analysis compares their substantive requirements and translates recurring principles into controls that can be implemented by SMEs without assuming the existence of dedicated AI governance departments. The resulting framework is conceptual rather than empirically validated; the proposed indicators are intended as practical monitoring devices rather than validated measurement scales.

2.2. Results and discussion

2.2.1. SME characteristics and AI governance requirements

The most important difference between SMEs and large firms concerns resource structure rather than technology itself. SMEs tend to favor ready-made tools, operate with limited budgets for independent audits, and rely on employees who perform several functions simultaneously. Data are often distributed across sales software, spreadsheets, e-commerce platforms, and external services. Accordingly, an appropriate governance approach should not simply replicate large-enterprise governance models; it should identify a limited set of controls that are proportionate, auditable, and feasible within existing organizational arrangements.

Table 1. SME characteristics and implications for AI governance

SME characteristic	Manifestation in AI use	Governance implication
Limited resources	Preference for ready-made tools; limited audit budgets	Prioritize controls for applications with significant risk
Multifunctional staff	Limited access to AI, data, and legal specialists	Assign roles and provide task-specific training
Fragmented data	Data distributed across multiple systems	Control provenance, quality, and access rights
Provider dependence	Use of external AI platforms	Review contractual terms, data practices, and incident handling
Lean governance	Few approval layers	Maintain records for material decisions and use cross-checks

Source: Author's synthesis based on OECD [1], [2].

2.2.2. Data governance gap

Data are the foundation of AI reliability, but data quality cannot be reduced to accuracy alone. Wang and Strong [10] argue that quality should be assessed in relation to the context of use, representation, and accessibility. In SMEs, data are often created before an AI application is defined and may therefore contain duplication, missing fields, inconsistencies across systems, or outdated information. If these limitations are not identified, they can be reproduced in AI outputs and subsequently affect business decisions.

Data governance should therefore cover the full lifecycle from collection and validation through storage, use, updating, and disposal. Gebru et al. [11] demonstrate the value of dataset documentation for recording provenance, purpose, composition, and limitations. For SMEs, this mechanism can be simplified into a data record containing the source, purpose, responsible person, access rights, retention period, and sharing conditions. Personal or confidential business data also require controls over the legal basis and conditions of use.

Table 2. Priority data-control points for SMEs

Control point	Minimum requirement
Provenance	Identify source, provider, and purpose of collection
Quality	Check accuracy, completeness, consistency, timeliness, and fitness for purpose
Use rights	Define access, sharing, retention, and deletion rights
Provider	Review retention, secondary use, access, and incident notification
Traceability	Retain sufficient information to identify the data and version used

Source: Developed by the author based on Wang and Strong [10], Gebru et al. [11], and NIST [5].

2.2.3. Gaps in transparency, explainability, and traceability

Transparency, explainability, and traceability are closely related but not interchangeable. Transparency provides information about the system's purpose, scope, operating conditions, and limitations; explainability concerns the basis of a particular output; traceability enables the organization to reconstruct relevant data, system versions, and the process through which a result was produced. The OECD principles call for meaningful information about AI capabilities, limitations, and factors relevant to predictions, recommendations, or decisions, while linking accountability to appropriate traceability [3].

For SMEs, transparency should not be interpreted as a requirement to disclose source code or force providers to reveal trade secrets. A more practical objective is to ensure that the organization knows what a tool is used for, what its limitations are, what data are processed, under

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

what conditions outputs are generated, and who is responsible for checking them. Low-impact applications may require only usage guidance and output checks; applications supporting material decisions require stronger documentation and traceability.

Table 3. Transparency and traceability by impact level

Impact level	Transparency and traceability requirements
Low	State purpose and limitations; check outputs
Moderate	Maintain a tool record, data source, version, and operating conditions
Significant	Retain appropriate input records, outputs, reviewer, approval basis, and review mechanism

Source: Developed by the author based on OECD [3], NIST [5], and Mitchell et al. [13]. The impact levels are analytical categories proposed in this study.

2.2.4. Accountability and human oversight gap

Accountability requires the organization to identify who is responsible, what evidence supports a decision, and how errors are handled. Multiple actors may participate in an AI chain, including providers, deploying organizations, users, and approvers. Kroll et al. [12] argue that algorithmic accountability must be supported by review mechanisms and procedural safeguards rather than relying solely on provider assurances.

For SMEs, a common weakness is the absence of clear rules about who may approve an AI tool, when outputs must be checked, and who receives incident reports. Human oversight should therefore mean a substantive capacity to intervene: an authorized person must have sufficient information, time, and authority to request a review, reject an output, or stop a process. One employee may perform several roles, but applications with significant impact should be subject to appropriate cross-checking or independent approval.

Table 4. Allocation of responsibilities in SME AI governance

Role	Core responsibility
Leadership	Approve objectives, policy, risk tolerance, and resources
AI/digital transformation coordinator	Manage the application inventory, monitoring, and assessment coordination
Data manager	Control provenance, quality, access, and data protection
User	Verify outputs, comply with rules, and report anomalies
Provider	Provide system information, data conditions, and incident support as agreed

Source: Developed by the author based on OECD [3], Kroll et al. [12], and NIST [5].

2.2.5. Proposed responsible AI governance framework

Drawing on international governance frameworks, the study proposes six complementary components. OECD provides principles concerning transparency, explainability, safety, and accountability; UNESCO emphasizes human rights, data governance, impact assessment, and education; NIST organizes AI risk management around Govern, Map, Measure, and Manage; and ISO/IEC 42001 establishes requirements for an AI management system [3]–[6]. The proposed framework is not presented as a statistically validated causal model. Rather, it is a governance structure that enables SMEs to translate these principles into manageable organizational controls.



Figure 1. Proposed responsible AI governance framework for SMEs.
Source: Developed by the author based on OECD [3], UNESCO [4], NIST [5], and ISO/IEC 42001 [6].

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

Table 5. Six components of the proposed responsible AI governance framework

Component	Core focus
Direction and commitment	Leadership defines purpose, scope, acceptable risk, and responsibility
Data governance	Control the data lifecycle, quality, use rights, access, and traceability
Transparency and explainability	Provide appropriate information on purpose, limitations, basis, and version
Accountability and oversight	Identify approvers and ensure the ability to review, reject, and stop processes
Risk and compliance	Scale controls to impact level; review legal and provider obligations
Capability and improvement	Provide task-specific training, record incidents, collect feedback, and update procedures

Source: Developed by the author based on OECD [3], UNESCO [4], NIST [5], and ISO/IEC 42001 [6].

The central principle of the framework is proportionality. SMEs should not apply the same level of control to every AI tool. An internal drafting application may require only usage rules and output review; a business forecasting application requires stronger controls over data and error; applications affecting employment, customer rights, or financial decisions require more intensive oversight, explanation, review, and record keeping. This approach is consistent with the risk-based orientation of NIST and the EU AI Act [5], [18].

The framework should operate as a continuous cycle: define purpose and scope; review data and the provider; assess risk; deploy with assigned responsibility; monitor outputs and incidents; and then adjust data, procedures, or conditions of use. Organizational maturity may be considered in three broad states—initial, integrated, and developing—but maturity should not replace risk classification. An organization at an early stage may still need strict controls when a particular application has significant consequences.

2.2.6. Operating mechanism and monitoring indicators

A governance framework has practical value only when it is translated into actions within business processes. For SMEs, the cycle can be organized into six recurring steps: define purpose and scope; check data and provider conditions; classify risk; deploy with an accountable person; monitor outputs and incidents; and review and improve. This cycle is compatible with the NIST risk-management approach [5] and the continual-improvement logic of management systems [6].

Maturity and application risk are distinct variables. An SME may not have a dedicated AI function but still needs strong controls for applications that can materially affect employees, customers, or partners. Conversely, a low-risk tool does not necessarily require a complex assessment. This distinction helps SMEs avoid both extremes: weak controls that create excessive dependence on AI outputs and burdensome controls that discourage useful adoption.

A small set of indicators can be used for monitoring. These indicators are not proposed as a validated performance scale; they are practical devices for converting governance requirements into information that can be reviewed periodically. Their selection should reflect the firm's sector, size, and data environment.

Table 6. Suggested indicators for monitoring AI governance in SMEs

Area	Suggested indicator	Recording method
Data	Share of applications with source records and quality checks	Compliant applications / total applications
Transparency	Share of applications with records of purpose, limitations, and provider	Applications with records / total applications
Accountability	Share of applications with an owner and, where required, an approver	Compliant applications / total applications
Oversight	Share of material outputs reviewed by humans	Reviewed outputs / controlled outputs
Incidents	Time from incident registration to closure	Incident log
Capability	Share of relevant employees completing training	Trained employees / relevant employees

Source: Proposed by the author based on NIST [5] and ISO/IEC 42001 [6].

These indicators can be recorded through spreadsheets or internal forms; a dedicated governance platform is not necessary. Their value lies in identifying recurring weaknesses, such as missing data records, applications without accountable owners, material outputs that have not been reviewed, or unresolved incidents. Repeated problems can then trigger adjustments to procedures, training, or provider contracts.

2.2.7. Legal context and implications for Vietnamese SMEs

The governance framework must be situated within the applicable legal environment. Decision No. 127/QD-TTg of 2021 established Vietnam's National Strategy on Research, Development and Application of Artificial Intelligence to 2030 [14]. The Law on Data No. 60/2024/QH15, effective from 1 July 2025, and the Law on Personal Data Protection No. 91/2025/QH15, effective from 1 January 2026, establish important requirements for data governance and processing [15], [16]. The Law on Artificial Intelligence No. 134/2025/QH15 was adopted on 10 December 2025 and took effect on 1 March 2026 [17].

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

For activities connected with the EU market, Regulation (EU) 2024/1689 establishes a risk-based regulatory approach and has a consolidated version updated on 27 July 2026 [18]. The regulation does not automatically apply to every Vietnamese SME, but it is directly relevant to organizations falling within its scope. International standards should therefore not be treated as blanket declarations of legal compliance; they are better used as references for internal controls, followed by assessment against the specific legal obligations applicable to the enterprise.

The proposed framework should also not be confused with a certification standard. ISO/IEC 42001 is an AI management system standard that can support organizations in establishing, maintaining, and improving an AI management system, whereas the framework proposed here is deliberately simplified so that SMEs can adopt it incrementally [6]. This distinction is important because small firms may otherwise attempt to reproduce governance arrangements that exceed their implementation capacity.

2.2.8. Discussion and research limitations

The analysis indicates that the most significant governance gap for SMEs is not necessarily a lack of technology but a lack of mechanisms for translating principles into explicit responsibilities and control activities. Data, transparency, and accountability are interdependent: data determine the basis for checking outputs; transparency enables people to understand and evaluate system behavior; and accountability ensures that an authorized person can intervene and correct errors. The six components therefore provide organizational conditions for managing these three core gaps.

The study contributes by connecting international AI governance frameworks with the resource constraints of SMEs rather than proposing a uniform governance model. Its limitations are equally important. The framework is derived from literature review and conceptual analysis and has not yet been tested through surveys, interviews, or operational data from SMEs. The proposed indicators and maturity states should therefore be regarded as provisional. Future research should test the framework across sectors, firm sizes, and AI applications, and examine whether the proposed controls improve measurable outcomes such as data quality, incident response, decision reliability, and stakeholder trust.

3. CONCLUSION AND RECOMMENDATIONS

3.1. Conclusion

The study identifies three central gaps in SME AI governance: data control, transparency and explainability, and accountability. These dimensions are mutually reinforcing and should be addressed through an integrated governance mechanism. Based on academic literature, OECD, UNESCO, NIST, ISO/IEC frameworks, and relevant legal instruments, the study proposes a six-component framework governed by a proportional, risk-based principle. The framework seeks to establish sufficient control, accountability, and human intervention without imposing governance structures disproportionate to SME resources.

3.2. Recommendations

For SMEs, immediate priorities should include a concise AI-use policy, an inventory of approved tools, rules for restricted data, designated responsibility, and approval requirements for higher-risk uses. Firms should maintain minimum records on data, providers, purposes, review results, and incidents. For material decisions, AI outputs should not be treated as the sole basis for action; authorized personnel must be able to review and reject them.

For regulators and business-support organizations, practical guidance designed specifically for SMEs should be developed, including model policies, data checklists, risk-assessment forms, and incident-response procedures. Digital-transformation support should be linked to training in data literacy, information security, and risk governance. AI providers should provide clear information on system functions and limitations, data processing, retention and deletion, system changes, and incident reporting. Such information can reduce the due-diligence burden faced by SMEs and strengthen their ability to exercise meaningful oversight.

REFERENCES

1) OECD (2025). AI Adoption by Small and Medium-Sized Enterprises: OECD Discussion Paper for the G7. OECD Publishing, Paris. https://doi.org/10.1787/426399c1-en.
2) Bianchini, M., Lasheras Sancho, M., & Larraín Aylwin, J. R. (2026). Empowering SMEs in the Age of AI: The 2026 OECD D4SME Survey. OECD SME and Entrepreneurship Papers, No. 78. OECD Publishing, Paris. https://doi.org/10.1787/bf5a9816-en.
3) OECD (2019, amended 2024). Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449. OECD Legal Instruments.
4) UNESCO (2021). Recommendation on the Ethics of Artificial Intelligence. UNESCO, Paris. https://unesdoc.unesco.org/ark:/48223/pf0000381137.
5) Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1.
6) ISO/IEC (2023). ISO/IEC 42001:2023 Information Technology—Artificial Intelligence—Management System. International Organization for Standardization.
7) Freeman, R. E. (1984). Strategic Management: A Stakeholder Approach. Pitman, Boston.
8) DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147–160. https://doi.org/10.2307/2095101.
9) Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic Management Journal, 18(7), 509–533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z.
10) Wang, R. Y., & Strong, D. M. (1996). Beyond accuracy: What data quality means to data consumers. Journal of Management Information Systems, 12(4), 5–33. https://doi.org/10.1080/07421222.1996.11518099.

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

11) Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Daumé III, H., & Crawford, K. (2021). Datasheets for datasets. Communications of the ACM, 64(12), 86–92. https://doi.org/10.1145/3458723.
12) Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. University of Pennsylvania Law Review, 165(3), 633–705.
13) Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., Spitzer, E., Raji, I. D., & Gebru, T. (2019). Model cards for model reporting. Proceedings of the Conference on Fairness, Accountability, and Transparency, 220–229. https://doi.org/10.1145/3287560.3287596.
14) Prime Minister of Vietnam (2021). Decision No. 127/QD-TTg dated 26 January 2021 approving the National Strategy on Research, Development and Application of Artificial Intelligence to 2030.
15) National Assembly of Vietnam (2024). Law on Data No. 60/2024/QH15 dated 30 November 2024, effective from 1 July 2025.
16) National Assembly of Vietnam (2025). Law on Personal Data Protection No. 91/2025/QH15 dated 26 June 2025, effective from 1 January 2026.
17) National Assembly of Vietnam (2025). Law on Artificial Intelligence No. 134/2025/QH15 dated 10 December 2025, effective from 1 March 2026.
18) European Parliament and Council of the European Union (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), current consolidated version 27 July 2026.
19) National Assembly of Vietnam (2017). Law on Support for Small- and Medium-Sized Enterprises No. 04/2017/QH14 dated 12 June 2017, effective from 1 January 2018.
20) Government of Vietnam (2021). Decree No. 80/2021/ND-CP dated 26 August 2021 detailing and guiding the implementation of certain provisions of the Law on Support for Small- and Medium-Sized Enterprises.

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

Corresponding Author: Ly Bich Ngoc