EUROPEAN INTERNATIONAL UNIVERSITY

AI Governance in the Age of Digital Transformation

A Practice-Oriented Framework for Ethical, Accountable, and ISO/IEC 42001-Aligned Artificial Intelligence

Saeed Alhawadi

MBA Candidate in Digital Transformation

European International University (EIU) – Paris | 2026

Email: saeedalhawadi94@gmail.com
LinkedIn: Saeed Alhawadi

EUROPEAN INTERNATIONAL UNIVERSITY

Contents

Abstract

Artificial intelligence (AI) has moved from pilot projects into core decisions, customer journeys, risk scoring, content generation, workforce planning, and public service design. Many organizations now face a governance gap: AI enters operations faster than accountability, control evidence, human oversight, and audit practice mature. This article addresses this gap through a practice-oriented framework for AI governance aligned with the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 42001 artificial intelligence management system. The article uses a design-oriented action research approach. It draws on academic literature, the European Union (EU) Artificial Intelligence Act, the Organisation for Economic Co-operation and Development (OECD) AI Principles, the National Institute of Standards and Technology (NIST) AI Risk Management Framework, and ISO/IEC 42001. Its contribution is the Governance Architecture for Trustworthy Enterprise AI (GATE-AI), an original framework for organizations undergoing digital transformation. GATE-AI translates ethical principles into decision rights, risk tiers, lifecycle gates, documentation artefacts, human oversight, monitoring routines, and management review. The proposed intervention supports AI inventory creation, risk classification, impact assessment, control treatment, release approval, incident learning, and continual improvement. Expected outcomes include stronger regulatory readiness, less shadow AI, clearer ownership, more reliable audit trails, improved stakeholder trust, and better alignment between digital transformation strategy and responsible AI practice. The article concludes by arguing for AI governance as a management discipline, not a compliance appendix.

Keywords: AI governance; digital transformation; responsible AI; ISO/IEC 42001; action research

1. Introduction and Context

Digital transformation has changed the place of AI in organizations. Earlier adoption often sat in analytics teams or experimental laboratories. Current adoption sits in customer service platforms, enterprise resource planning, marketing automation, recruitment tools, credit decisions, cybersecurity operations, and generative AI assistants used by employees every day. This shift creates value when AI improves speed, consistency, discovery, and service quality. It also creates exposure when automated outputs affect rights, safety, access to opportunity, privacy, reputation, or public trust.

The management issue is practical. Organizations often approve AI projects through technology budgets, procurement channels, or informal business experiments. Risk functions, legal teams, data protection officers, internal audit, and affected business units enter late, after design decisions already shape data, model behavior, vendor dependence, and user expectations. Digital transformation then produces an accountability gap. Leaders seek innovation, yet evidence about AI purpose, risk classification, data lineage, fairness testing, human oversight, monitoring, and escalation remains fragmented.

This article treats AI governance as a discipline of organizational change. Policies matter, yet policy language alone does not govern an AI system. Governance appears when leaders define decision rights, assign ownership, create repeatable controls, require evidence at release gates, monitor real-world behavior, and learn from incidents. This orientation aligns with action research because it asks managers to diagnose a real organizational problem, test an intervention, observe effects, and refine practice through reflection.

The organizational context used for the proposed intervention is a medium-to-large service organization in active digital transformation. Such an organization uses cloud platforms, vendor AI tools, customer analytics, process automation, and generative AI for knowledge work. It has existing corporate governance, information technology

governance, data governance, privacy, cybersecurity, procurement, and audit functions. Yet it lacks an integrated AI Management System (AIMS) able to connect those functions around AI-specific risks.

2. Research Problem and Objectives

The research problem is the gap between rapid AI adoption and mature AI governance. Organizations need speed, yet AI risks often unfold through complex socio-technical interactions. A recruitment model reflects historical data, labor market patterns, user interpretation, and workflow incentives. A generative AI assistant reflects model provider choices, prompt design, retrieval sources, privacy controls, and employee judgment. A fraud detection model reflects risk appetite, false positive tolerance, customer communication, and appeal procedures. In each case, the technical system and the organization act together.

The central problem is not the absence of ethical principles. Most organizations already endorse fairness, transparency, accountability, security, and privacy. The problem is translation. Ethical words need managerial forms: a register, a risk owner, a review forum, a test plan, a release gate, an exception process, user instructions, incident logs, and periodic management review. Without these forms, AI governance remains symbolic. It looks respectable in presentations but fails under operational pressure.

This article has four objectives. First, it synthesizes current AI governance literature and standards relevant to practice. Second, it compares the governance logic of the EU AI Act, OECD AI Principles, NIST AI Risk Management Framework, and ISO/IEC 42001. Third, it proposes an original ISO/IEC 42001-aligned framework named GATE-AI. Fourth, it describes an intervention path for organizations seeking to embed AI governance in digital transformation rather than attaching it after deployment.

The article also aims to support managers who need a usable bridge between board-level concern and delivery-team action. The intended audience includes executives, digital transformation leaders, risk managers, data and AI teams, legal and compliance staff, procurement teams, internal auditors, and academic practitioners interested in action research.

3. Literature Review

Digital transformation research explains technology change as more than digitization of existing processes. It involves shifts in value creation, organizational structures, roles, skills, and strategic response (Vial, 2019). AI intensifies this shift because AI systems learn from data, operate with degrees of autonomy, and produce outputs less transparent than many earlier information systems. Managing AI therefore requires attention to autonomy, learning, and opacity, along with coordination across business and technical functions (Berente et al., 2021).

AI governance scholarship has moved from principles toward organizational implementation. Mantymaki et al. (2022) define organizational AI governance as the means through which organizations direct, control, and coordinate AI in line with goals and values. Batool et al. (2025) find gaps in who governs, what is governed, when governance occurs, and how mechanisms operate across the AI lifecycle. Papagiannidis et al. (2025) place responsible AI governance in structural, relational, and procedural practices. These studies support a practical claim: governance needs organization design, not only ethical aspiration.

The literature also warns against technical reductionism. Fairness, for example, is not solved by selecting one metric in isolation. Selbst et al. (2019) argue for a socio-technical view because fairness choices meet institutional rules, user behavior, historical disadvantage, and legal duties. This matters for managers. A model with acceptable validation scores still produces harm if deployed in a poor workflow, explained badly, monitored weakly, or used outside its intended context.

Documentation and auditability form a second line of scholarship. Model cards describe purpose, performance, limitations, and evaluation results (Mitchell et al., 2019). Datasheets for datasets record dataset motivation, composition, collection, and recommended uses (Gebru et al., 2021). Internal algorithmic auditing places evidence across the development lifecycle and links audit practice with organizational values (Raji et al., 2020). These artefacts do not replace governance, yet they supply the evidence needed for review, assurance, and learning.

A recurring limitation in practice is fragmentation. Data governance focuses on data quality and access. Cybersecurity focuses on threat control. Privacy teams focus on lawful processing. Procurement focuses on vendor terms. Business owners focus on outcomes. AI governance must connect these domains and add AI-specific questions: intended use, autonomy level, human oversight design, model evaluation, bias risk, model drift, explainability, user reliance, third-party model dependence, and decommissioning.

4. Theoretical Foundations of AI Governance

The first foundation is socio-technical systems thinking. AI systems operate through people, data, models, incentives, interfaces, processes, and institutions. Governance therefore needs attention to workflow, authority, training, and escalation. A high-risk decision support tool is not safe because a model performs well in a test set. It becomes safer when users understand limits, managers define accountability, performance is monitored, and affected persons receive explanations and appeal routes.

The second foundation is risk-based governance. Not all AI use deserves the same level of control. A grammar assistant in a low-risk internal task differs from an AI system used for hiring, lending, medical triage, or public benefits. Risk-based governance uses tiering to allocate effort. Low-risk uses receive baseline rules and user guidance. Medium-risk uses receive documentation, testing, and owner review. High-risk uses require formal impact assessment, independent challenge, legal review, human oversight, post-deployment monitoring, and management sign-off.

The third foundation is accountability by design. Accountability means identifiable persons and bodies hold duties before, during, and after AI deployment. It also means evidence exists to support review. A governance council without a system owner leaves accountability vague. A system owner without an evidence record lacks assurance. A model validation report without incident reporting misses real use. Accountability by design links roles, decisions, records, and consequences.

The fourth foundation is the management system approach. ISO/IEC 42001 follows a management system logic: establish policy and objectives, implement processes,

evaluate performance, and improve over time (ISO & IEC, 2023). This approach suits AI because AI systems change after deployment through data drift, model updates, vendor changes, user feedback, and new regulation. Governance therefore needs continual improvement, not one-time approval.

5. Global AI Governance Frameworks and Standards

The EU AI Act creates a risk-based legal structure for AI systems placed on the market, put into service, or used in the EU. The regulation distinguishes unacceptable-risk AI practices, high-risk AI systems, transparency obligations, and other lower-risk uses (European Parliament and Council of the European Union, 2024). The European Commission describes the Act as a uniform framework across EU countries with duties for developers and deployers, including requirements for high-risk systems such as risk mitigation, data quality, information for users, and human oversight (European Commission, 2024). General-purpose AI (GPAI) obligations include technical documentation, a copyright policy, and a public summary of training content, with additional duties for GPAI models with systemic risk (European Commission, 2025).

The OECD AI Principles provide a values-based foundation for trustworthy AI. The principles cover inclusive growth, human rights and democratic values, transparency and explainability, safety and security, and accountability. The 2024 update addressed general-purpose and generative AI concerns, including privacy, intellectual property, safety, and information integrity (OECD, 2024a, 2024b). The OECD contribution is important because it supplies a shared policy vocabulary used by governments and international bodies.

The NIST AI Risk Management Framework (AI RMF) is voluntary and organized around Govern, Map, Measure, and Manage functions (NIST, 2023). Its value for organizations lies in operational detail. Govern sets culture, policies, and accountability. Map clarifies context, stakeholders, intended use, and impacts. Measure tests and evaluates risk. Manage prioritizes treatment and monitoring. NIST AI 600-1 extends this logic to generative AI and identifies risks such as confabulation, data leakage, cybersecurity vulnerability, information integrity, and misuse (NIST, 2024).

ISO/IEC 42001 is the first certifiable management system standard for AI. It applies to organizations developing, providing, or using AI-based products and services and requires an AIMS for responsible AI governance (ISO & IEC, 2023). ISO describes the AIMS as a set of related organizational elements for policies, objectives, and processes linked to responsible AI development, provision, or use. ISO/IEC 23894 complements this standard by giving AI-specific risk management guidance for organizations involved with AI products, systems, and services (ISO & IEC, 2023a, 2023b).

Together, these frameworks create a layered governance architecture. The EU AI Act sets enforceable duties for relevant contexts. The OECD principles define values and policy direction. NIST supplies a risk management playbook. ISO/IEC 42001 supplies a management system for institutionalizing controls and improvement. An organization seeking practical AI governance needs to combine these resources rather than select one in isolation.

Table 1. Complementary logic of major AI governance frameworks

Framework or standard	Primary contribution for organizational practice
EU AI Act	Legal risk classification, duties for high-risk systems, transparency duties, and GPAI obligations for relevant actors.
OECD AI Principles	Shared values for trustworthy AI, including human rights, transparency, safety, and accountability.
NIST AI RMF	Risk management functions for governance, mapping, measurement, and treatment of AI risks.
ISO/IEC 42001	AIMS requirements for policy, objectives, operational controls, performance evaluation, audit, and continual improvement.

6. Methodology and Approach

This article uses a practice-based design and action research orientation. Action research in business and management emphasizes actionable knowledge, reflection, and change in organizational settings (Coghlan & Shani, 2019). The approach suits AI governance because the problem is not only analytical. It is a change problem involving leadership, teams, tools, incentives, documentation, training, and assurance.

The methodology has four steps. The first step diagnoses the organizational governance gap through a review of AI use cases, existing policies, risk procedures,

procurement processes, privacy controls, security controls, and audit practices. The second step designs an intervention aligned with global frameworks and ISO/IEC 42001. The third step applies the intervention to selected AI use cases across risk tiers. The fourth step reflects on outcomes through management review, lessons learned, and updates to controls.

The approach is conceptual and practice-oriented rather than empirical field reporting. No human participant data is collected. The proposed intervention is intended for adaptation by organizations in finance, education, public administration, healthcare support, logistics, retail, and professional services. The framework is also suitable for organizations using vendor AI services, internally developed models, or generative AI tools embedded in enterprise platforms.

Evidence in this methodology consists of governance artefacts. Examples include an AI inventory, use-case intake forms, risk tiering records, data documentation, model cards, vendor due diligence records, impact assessments, approval minutes, testing reports, user instructions, monitoring dashboards, incident reports, and management review outputs. These artefacts matter because they turn governance into observable work.

7. Action or Intervention: The GATE-AI Framework

The original contribution of this article is the Governance Architecture for Trustworthy Enterprise AI (GATE-AI). GATE-AI is a practice-oriented framework aligned with ISO/IEC 42001 and compatible with the EU AI Act, OECD AI Principles, and NIST AI RMF. It is designed for organizations undergoing digital transformation, especially those needing a single operating model for ethical, accountable, transparent, and compliant AI.

GATE-AI has four stages. Ground establishes governance scope, leadership commitment, AI policy, an AI inventory, risk appetite, and role accountability. Assess classifies AI use cases, maps stakeholders, performs risk and impact assessment, and identifies legal, ethical, security, privacy, and operational requirements. Treat defines controls, lifecycle gates, human oversight, testing, vendor obligations, documentation,

and release criteria. Evolve monitors performance, detects incidents, reviews control effectiveness, audits evidence, and improves the AIMS through management review.

The framework uses decision gates across the AI lifecycle. Gate 0 records idea intake and business purpose. Gate 1 checks permissibility, risk tier, and strategic fit. Gate 2 reviews design, data, vendor, and human oversight. Gate 3 approves pre-deployment assurance, including testing and legal review. Gate 4 monitors live use, incidents, drift, complaints, and user reliance. Gate 5 governs major change, retirement, or replacement. Each gate has an accountable owner, minimum evidence, and escalation path.

GATE-AI also uses five evidence objects. The AI Use-Case Register records purpose, owner, vendor, data sources, autonomy level, user group, and risk tier. The Risk and Rights Impact Log records harms, affected stakeholders, legal triggers, and treatment decisions. The Control Plan records safeguards, testing, human oversight, security, privacy, transparency, and monitoring. The Accountability Matrix uses Responsible, Accountable, Consulted, and Informed (RACI) roles for each decision gate. The Assurance Dashboard reports Key Performance Indicators (KPIs), incidents, exceptions, audit findings, and improvement actions.

Table 2. GATE-AI stages and ISO/IEC 42001 alignment

GATE-AI stage	Core practice and evidence
Ground	Define scope, AI policy, risk appetite, AI inventory, leadership commitment, and accountable roles.
Assess	Classify use cases, map stakeholders, assess risks and impacts, and identify legal and ethical duties.
Treat	Apply controls, lifecycle gates, testing, human oversight, documentation, vendor obligations, and release approval.
Evolve	Monitor live systems, record incidents, run internal audit, hold management review, and improve the AIMS.

8. Framework Components, Roles, Controls, and Outcomes

The governance roles in GATE-AI reflect both leadership and delivery. The board or executive committee approves AI risk appetite and receives periodic assurance. The AI Governance Council reviews high-risk use cases and policy exceptions. The executive

AI sponsor funds the AIMS and resolves cross-functional barriers. The AI system owner is accountable for purpose, risk tier, approval, monitoring, and retirement. Data stewards manage data quality, lineage, and access. Security, privacy, legal, procurement, and compliance teams review domain-specific risks. Internal audit examines evidence and control maturity.

Technical teams retain responsibility for design integrity. Data scientists, machine learning engineers, product owners, and solution architects prepare documentation, testing, and monitoring plans. Business process owners define the operational context and decide acceptable error tolerance. Human reviewers perform oversight in high-impact decisions. User representatives and affected stakeholder proxies help identify foreseeable harm. Vendor managers ensure external providers meet documentation, audit, security, and incident notification duties.

Risk controls are organized by lifecycle. Planning controls include AI policy, use-case intake, role assignment, and risk classification. Design controls include data suitability assessment, privacy review, fairness analysis, security threat modelling, and human oversight design. Build controls include model documentation, version control, testing, reproducibility, and change management. Deployment controls include release approval, user training, transparency notices, fallback processes, and complaint routes. Operation controls include monitoring, drift detection, incident response, periodic revalidation, and decommissioning.

Expected outcomes are both compliance-oriented and transformational. Compliance outcomes include better alignment with legal duties, ISO/IEC 42001 readiness, audit evidence, and management review. Ethical outcomes include clearer responsibility for fairness, privacy, human oversight, transparency, and contestability. Business outcomes include less duplication, faster review of low-risk uses, fewer uncontrolled tools, improved vendor discipline, and stronger trust in AI-enabled digital transformation.

9. ISO/IEC 42001 Alignment

GATE-AI aligns with ISO/IEC 42001 through the management system cycle. Ground corresponds to context, leadership, policy, scope, and AI objectives. Assess

corresponds to planning, AI risk assessment, opportunity assessment, and stakeholder requirements. Treat corresponds to operational controls, competence, communication, documented information, and AI lifecycle management. Evolve corresponds to performance evaluation, internal audit, management review, corrective action, and continual improvement.

This alignment is important because ISO/IEC 42001 changes the governance conversation from ethical preference to accountable management practice. An organization seeking certification or internal assurance needs evidence of policy, objectives, procedures, competence, risk treatment, monitoring, audit, and improvement. GATE-AI gives managers a structure for producing this evidence in a way linked to real AI systems, not a generic compliance manual.

ISO/IEC 42001 also encourages integration with existing management systems. Many organizations already operate information security, privacy, quality, business continuity, or risk management systems. AI governance should not duplicate them. GATE-AI connects with those systems through shared evidence and decision gates. Security teams manage adversarial and access risks. Privacy teams review lawful basis and data minimization. Quality teams review process conformance. Internal audit reviews control effectiveness. The AIMS coordinates these contributions for AI-specific accountability.

The practical challenge is proportionality. A small internal productivity assistant does not require the same assurance package as a high-risk credit or employment system. GATE-AI therefore uses risk tiering, minimum evidence by tier, and escalation rules. This keeps governance practical, protects innovation, and directs attention toward applications with higher impact.

10. Findings or Expected Outcomes

Since this article develops a practice framework rather than reporting completed field results, findings are framed as expected outcomes from implementation. The first expected outcome is visibility. An AI inventory provides leaders with a reliable view of systems in use, owners, vendors, data sources, risk tiers, and monitoring status.

Visibility is the starting point for governance because unknown AI systems escape policy, training, audit, and incident response.

The second expected outcome is accountability. GATE-AI assigns an accountable system owner and gate-specific responsibilities. This reduces the common situation in which technology teams, business teams, legal teams, and vendors each assume another party owns the final risk decision. Accountability becomes explicit through the RACI matrix, approval records, exception logs, and management review.

The third expected outcome is better decision quality. Risk classification separates low-risk productivity uses from high-impact decisions. This prevents over-control of routine uses and under-control of sensitive uses. It also gives delivery teams earlier guidance about required testing, documentation, human oversight, and transparency. Earlier guidance reduces late-stage redesign and improves trust between innovation teams and control functions.

The fourth expected outcome is audit readiness. Model cards, datasheets, impact logs, control plans, monitoring dashboards, and incident reports create a traceable evidence chain. This evidence supports internal audit, regulatory engagement, ISO/IEC 42001 readiness, and board reporting. The organization becomes better prepared to explain why an AI system exists, how it was approved, what risks were accepted, and how live performance is reviewed.

The fifth expected outcome is organizational learning. Incidents, complaints, drift reports, and audit findings are not treated as failures to hide. They become input for corrective action, policy refinement, model change, user training, and improved procurement. This is the action research value of GATE-AI: governance improves through cycles of action and reflection.

11. Reflection and Implications for Practice

The main reflection from this work is straightforward: AI governance succeeds when it becomes part of ordinary management. It fails when treated as a document written for regulators or as a technical review owned only by data scientists. Managers need to see

AI governance as a shared operating model, similar to financial control, safety management, information security, or quality assurance.

A second reflection concerns speed. Many teams resist governance because they expect delay. Poor governance does delay projects, especially when requirements appear late. Good governance accelerates responsible delivery by clarifying evidence needs early. A low-risk use receives a light path. A high-risk use receives early review before design choices harden. A prohibited or unacceptable use is stopped before resources are wasted.

A third reflection concerns culture. AI governance requires psychological safety for raising concerns. Employees should be able to question data quality, model limitations, vendor claims, user reliance, or possible discrimination. Leadership must treat these concerns as part of professional practice. A culture focused only on deployment speed invites under-reporting. A culture focused only on risk avoidance blocks digital transformation. GATE-AI seeks disciplined innovation between these extremes.

For practitioners, the implications are concrete. Start with an inventory. Name accountable owners. Classify use cases by risk. Define minimum evidence by tier. Build lifecycle gates into existing project, procurement, and change-management processes. Train employees on responsible use. Monitor live systems. Review incidents and exceptions. Report performance to executives. Improve the AIMS after each review cycle.

12. Ethical, Legal, and Regulatory Challenges

Ethical challenges include bias, discrimination, manipulation, loss of agency, opacity, exclusion, and over-reliance on automated outputs. These risks are especially acute in employment, finance, education, healthcare, insurance, policing, migration, and public services. Ethical review should examine affected groups, foreseeable misuse, severity of harm, reversibility, ability to contest decisions, and availability of human support.

Legal challenges include data protection, intellectual property, consumer protection, employment law, sector regulation, cybersecurity duties, product safety, contract liability, and cross-border data transfers. The EU AI Act adds AI-specific duties for

organizations in scope, especially for high-risk systems and GPAI providers or deployers. Legal review should not occur after technical design. It should occur at Gate 1 and Gate 2, when purpose, data, vendor choice, and human oversight remain open for design change.

Regulatory challenges are complicated by jurisdictional overlap. A global organization might use one AI service across multiple regions, each with different privacy, safety, discrimination, and transparency duties. Vendor contracts might shift responsibility, but they do not remove organizational accountability for deployment choices. GATE-AI therefore requires vendor due diligence, contractual documentation duties, audit rights, incident notification, data-use restrictions, and exit plans.

Generative AI adds further challenges. Outputs might contain false statements, sensitive information, copyrighted content, unsafe advice, or manipulated instructions. NIST AI 600-1 highlights risks related to generative AI such as confabulation, information integrity, data leakage, and misuse (NIST, 2024). Organizations need clear rules for approved tools, prohibited uses, confidential data, review of generated content, prompt logging, and incident escalation.

13. Risk Management, Accountability, Transparency, and Compliance

Risk management under GATE-AI begins with purpose. No AI system should proceed without a clear business purpose, owner, intended users, affected stakeholders, autonomy level, data sources, and success criteria. Purpose controls scope creep. It also helps reviewers judge whether AI is proportionate, lawful, and aligned with organizational values. A vague purpose such as improve efficiency is insufficient for high-impact systems.

Risk assessment should cover technical, ethical, legal, operational, security, privacy, and reputational risk. It should include likelihood, severity, detectability, affected stakeholder groups, reversibility, and available safeguards. AI risk assessment should also include model-specific risk such as drift, bias, explainability limits, adversarial vulnerability, data leakage, and reliance on third-party models. ISO/IEC 23894 supports

such integration of AI-specific risk into organizational risk management (ISO & IEC, 2023b).

Accountability requires named decision makers. The AI Governance Council should approve high-risk systems and exceptions. The system owner should accept residual risk. Legal, security, privacy, and compliance teams should provide domain opinions. Technical teams should attest to validation and monitoring readiness. Internal audit should review evidence independently. This distributed model avoids false accountability, where everyone is involved and no one is accountable.

Transparency should be operational, not performative. Users need clear information about AI involvement, purpose, limitations, human review, and complaint routes. Internal stakeholders need model documentation, data documentation, approval history, risk treatment, and monitoring results. External stakeholders need explanations suited to context, especially when AI affects access, opportunity, safety, or rights. Transparency also means keeping records sufficient for audit and regulatory review.

Compliance requires continuous alignment. The organization should maintain a control library mapped to legal duties, ISO/IEC 42001 requirements, NIST AI RMF functions, OECD principles, and internal policy. A change in model provider, data source, intended use, geography, or user group should trigger reassessment. Compliance is not a one-time approval. It is a living process tied to the lifecycle of each AI system.

Table 3. Minimum evidence by AI risk tier

Risk tier	**Minimum governance evidence**
Low	Owner, purpose, approved tool, basic user guidance, and acceptable-use record.
Medium	AI register entry, data review, model or vendor documentation, testing record, transparency note, and owner sign-off.
High	Impact assessment, legal and privacy review, security review, human oversight plan, validation report, council approval, monitoring dashboard, incident plan, and periodic revalidation.
Prohibited or unacceptable	Stop decision, rationale, escalation record, and communication to requester.

14. Future Directions and Policy Recommendations

Organizations should elevate AI governance to board and executive agendas. AI oversight should be linked with enterprise risk management, digital transformation strategy, cybersecurity, privacy, and internal audit. Boards should receive concise dashboards covering AI inventory, high-risk systems, incidents, exceptions, audit findings, and regulatory exposure. Executive teams should fund AIMS capabilities, including skilled governance staff and tooling.

Policy makers should promote interoperability. Organizations face difficulty when guidance arrives as separate checklists with different vocabulary. Regulators and standards bodies should publish crosswalks, shared templates, and sector examples. This would reduce duplication and help smaller organizations implement meaningful controls without excessive administrative burden. Regulatory sandboxes should include governance evidence, not only technical prototypes.

Professional education should develop AI governance translators. These professionals understand AI, law, ethics, risk, audit, process design, and change management. They do not need to replace data scientists or lawyers. They connect disciplines. Digital transformation programs should teach students how to build an AI inventory, run an impact assessment, design human oversight, review vendor claims, and prepare management review evidence.

Organizations using GPAI should create specialized controls. These include approved-tool lists, prompt and output handling rules, restrictions on confidential data, human review for high-impact outputs, source verification, intellectual property checks, red-team testing for sensitive applications, and incident reporting. As generative AI becomes embedded in enterprise software, governance must move from optional guidance to operational control.

Future research should test GATE-AI in live organizations. Useful studies would compare implementation in regulated and less regulated sectors, measure the effect of risk tiering on project speed, examine employee adoption of generative AI rules, and evaluate whether ISO/IEC 42001 certification improves governance maturity. Action

research is well suited to such work because it values intervention, reflection, and learning in real organizational settings.

15. Conclusion

AI governance in digital transformation is now an organizational necessity. The central challenge is translating principles, laws, and standards into daily decisions. Organizations need more than statements about ethical AI. They need inventories, owners, risk tiers, impact assessments, lifecycle gates, documentation, monitoring, audits, incident learning, and management review.

This article proposed GATE-AI as an original, practice-oriented framework aligned with ISO/IEC 42001. The framework combines the legal discipline of the EU AI Act, the values of the OECD AI Principles, the risk functions of the NIST AI RMF, and the management system logic of ISO/IEC 42001. It offers an implementable path for organizations seeking ethical, accountable, transparent, and compliant AI during digital transformation.

The broader contribution is a shift in perspective. AI governance should not be seen as a barrier to innovation. It is the management infrastructure needed for trustworthy innovation. When governance is proportionate, evidence-based, and integrated with existing organizational processes, it supports responsible speed. It helps leaders know what AI exists, who owns it, what risks are accepted, what controls operate, and how the organization learns.

16. Ethical Approval, Declarations, and AI-Use Disclosure

Ethical approval and consent: Not applicable. This article is a conceptual and practice-oriented research article using publicly available literature, standards, and regulatory sources. It does not involve human participants, personal data collection, interviews, surveys, or experiments.

Conflict of interest statement: The author declares no conflict of interest.

Funding statement: No external funding was received for this manuscript.

AI-use disclosure statement: AI tools were used to support language editing, structure, and clarity. The author reviewed, verified, and approved the final manuscript before submission. Responsibility for accuracy, originality, citations, and final content remains with the author.

Copyright and author declaration: This work is original, has not been published previously, and is not under consideration by another journal or publisher. All sources are properly cited and referenced. The author retains authorship credit. The manuscript is suitable for open-access academic publication, subject to journal review and author approval.

References

Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: A systematic literature review. AI and Ethics, 5, 3265-3279. https://doi.org/10.1007/s43681-024-00653-w

Berente, N., Gu, B., Recker, J., & Santhanam, R. (2021). Managing artificial intelligence. MIS Quarterly, 45(3), 1433-1450. https://doi.org/10.25300/MISQ/2021/16274

Coghlan, D., & Shani, A. B. (2019). Action research in business and management: A reflective review. Action Research, 17(3), 518-541. https://doi.org/10.1177/1476750319852147

European Commission. (2024). AI Act enters into force. https://commission.europa.eu/news-and-media/news/ai-act-enters-force-2024-08-01_en

European Commission. (2025). General-purpose AI obligations under the AI Act. https://digital-strategy.ec.europa.eu/en/factpages/general-purpose-ai-obligations-under-ai-act

European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying

down harmonised rules on artificial intelligence. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Daume III, H., & Crawford, K. (2021). Datasheets for datasets. Communications of the ACM, 64(12), 86-92. https://doi.org/10.1145/3458723

High-Level Expert Group on Artificial Intelligence. (2019). Ethics guidelines for trustworthy AI. European Commission. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

International Organization for Standardization and International Electrotechnical Commission. (2023a). ISO/IEC 42001:2023, Artificial intelligence, Management system. ISO. https://www.iso.org/standard/42001

International Organization for Standardization and International Electrotechnical Commission. (2023b). ISO/IEC 23894:2023, Artificial intelligence, Guidance on risk management. ISO. https://www.iso.org/standard/77304.html

Mantymaki, M., Minkkinen, M., Birkstedt, T., & Viljanen, M. (2022). Defining organizational AI governance. AI and Ethics, 2, 603-609. https://doi.org/10.1007/s43681-022-00143-x

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

National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

National Institute of Standards and Technology. (2024). Artificial intelligence risk management framework: Generative artificial intelligence profile (NIST AI 600-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.600-1

Organisation for Economic Co-operation and Development. (2024a). OECD AI Principles overview. https://oecd.ai/en/ai-principles

Organisation for Economic Co-operation and Development. (2024b). OECD updates AI Principles to stay abreast of rapid technological developments. https://www.oecd.org/en/about/news/press-releases/2024/05/oecd-updates-ai-principles-to-stay-abreast-of-rapid-technological-developments.html

Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. Journal of Strategic Information Systems, 34(2), 101885. https://doi.org/10.1016/j.jsis.2024.101885

Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 33-44. https://doi.org/10.1145/3351095.3372873

Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and abstraction in socio-technical systems. Proceedings of the Conference on Fairness, Accountability, and Transparency, 59-68. https://doi.org/10.1145/3287560.3287598

UNESCO. (2021). Recommendation on the ethics of artificial intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000381137

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. Journal of Strategic Information Systems, 28(2), 118-144. https://doi.org/10.1016/j.jsis.2019.01.003