American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Board Oversight of Generative Artificial Intelligence Use

Dr. Roberto Santoro

Senior Lecturer, University of Genoa, Italy

Abstract

Generative Artificial Intelligence is expanding from experimental technology into organizational applications involving analysis, communication, software development, knowledge retrieval, forecasting support, document preparation, and decision assistance. Its accessibility creates an unusual governance challenge because adoption can occur rapidly through both centrally approved systems and decentralized employee use. Boards of directors are therefore required to understand not only the strategic opportunities associated with generative models but also whether management has established suitable boundaries for data protection, model reliability, intellectual-property exposure, cybersecurity, human accountability, third-party dependence, and escalation of material incidents. This study develops a board-level governance framework for overseeing organizational use of Generative Artificial Intelligence without transferring operational model management to directors. Because authenticated corporate board data were not supplied, the quantitative component is explicitly structured as a simulation-based methodological study. Seventy-two synthetic board-governance profiles are evaluated across six generative-AI use scenarios, producing 432 simulated board-risk assessments.

A Board Generative AI Oversight Maturity Index is developed from six dimensions: strategic authorization, use-case visibility, data and intellectual-property governance, model-risk control, human accountability, and monitoring and escalation readiness. A complementary Generative AI Risk Recognition Score evaluates whether boards identify and prioritize material risks arising from proposed organizational use. Simulated analysis indicates that recognition performance increases from 48 points under ad hoc adoption to 90 points under assured and adaptive oversight. The study argues that effective board oversight should neither consist of passive reliance on management nor involve directors approving individual prompts and model configurations. Instead, boards should establish risk appetite, require transparent inventories of material applications, clarify accountable ownership, demand reliable assurance information, and ensure that significant incidents can be escalated. The framework provides a testable basis for future empirical research on board governance of generative technologies.

Keywords: Generative Artificial Intelligence, board oversight, corporate governance, AI governance, model risk, digital risk, responsible AI, board accountability

1. Introduction

Generative Artificial Intelligence has created a distinctive governance problem because sophisticated computational capabilities can be introduced into organizations with substantially less infrastructure than

many earlier enterprise technologies. Large language and foundation-model systems can generate text, software code, summaries, classifications, analytical narratives, and other outputs from relatively simple user instructions. Research on large-scale language models established that sufficiently scaled models could perform diverse tasks with limited task-specific adaptation, while subsequent foundation-model research highlighted both their broad downstream utility and the possibility that weaknesses in general-purpose models may be inherited across many applications. This combination of versatility and scalability means that generative systems can move from experimentation to business use faster than conventional governance processes are accustomed to managing.

For boards of directors, the issue is not whether directors should become model engineers. Corporate boards traditionally perform direction, monitoring, and advisory functions, while management retains responsibility for execution. Hilb's analysis of artificial intelligence in corporate governance similarly distinguishes different levels at which AI may assist, augment, or potentially reshape board activity and argues that directors must take an active role in understanding and shaping the governance implications of intelligent systems. Research on digital transformation also emphasizes that boards require sufficient structures, processes, and information to govern strategically significant technology rather than leaving technology oversight exclusively to operational specialists. Generative AI therefore belongs within corporate governance when its use can materially affect strategy, reporting, customers, employees, intellectual property, regulatory compliance, cybersecurity, or corporate reputation.

The governance challenge is intensified by the characteristics of generative models themselves. A system may produce fluent output without guaranteeing factual correctness, may reproduce undesirable patterns present in training information, and may expose organizations to problems involving sensitive information, harmful content, misuse, or inappropriate reliance. Bender and colleagues identified substantial social and informational risks associated with increasingly large language models, while Weidinger and colleagues organized language-model risk into areas including discrimination, information hazards, misinformation, malicious use, interaction harms, and broader automation effects. NIST's explainability work further emphasizes that meaningful explanations, accurate representation of system processes, and operation within appropriate knowledge limits are important elements of trustworthy AI. These characteristics imply that conventional technology approval may be insufficient where employees can rely on model outputs in contexts substantially different from those originally intended.

Board oversight must therefore address two opposing governance failures. The first is under-governance, in which organizations adopt generative systems without a clear inventory, risk classification, ownership structure, or escalation mechanism. The second is over-centralization, in which boards become involved in technical or operational decisions that properly belong to management. Enterprise-risk principles provide a useful boundary: boards should understand major organizational risks, consider them in relation to risk appetite, and determine whether management's responses are appropriate rather than directly administering individual controls. In the AI context, Hickman and Petrin similarly connect trustworthy-AI requirements with corporate leadership, human intervention, robustness, data governance, and intra-corporate oversight.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

2. Objectives of the Study

2.1 To Develop a Board-Level Generative AI Oversight Framework

The first objective is to define the governance responsibilities that become relevant when generative systems are used within an organization. The framework distinguishes board oversight from operational AI management. Directors are expected to understand strategically important use cases, approve an appropriate risk appetite, question whether management has established suitable control architecture, and obtain assurance concerning material exposures. They are not expected to review ordinary prompts, retrain models, or approve every employee application.

The proposed framework therefore focuses on governance mechanisms that remain meaningful at board level: strategic authorization, organizational visibility over use, information and intellectual-property safeguards, model-risk controls, assignment of accountable executives, and monitoring and escalation. This separation is essential because effective oversight requires sufficient depth to challenge management without confusing governance with execution.

2.2 To Measure Generative AI Oversight Maturity

The second objective is to operationalize board oversight through a multidimensional maturity measure. A board that receives an annual presentation on artificial intelligence cannot automatically be regarded as exercising effective oversight if directors lack information concerning which systems are in use, what information enters those systems, which decisions rely on their outputs, and what happens when a significant problem occurs.

The study consequently proposes a Board Generative AI Oversight Maturity Index that evaluates whether governance processes are embedded rather than merely documented. Higher maturity requires board-level awareness of material applications, clearly assigned management ownership, regular reporting, defined risk thresholds, independent or second-line challenge where appropriate, and escalation of material incidents.

2.3 To Evaluate Emerging Risk Recognition Under Different Oversight Conditions

The third objective is to examine whether stronger oversight architecture improves simulated recognition of generative-AI-related risks. Recognition is treated as the board's capacity to identify which aspects of a proposed use case deserve governance attention rather than the technical ability to predict individual model failures.

Six use scenarios are therefore used to test whether synthetic boards recognize risks involving confidential information, unreliable content, bias, intellectual-property exposure, cybersecurity, third-party concentration, weak human review, and reporting integrity. The analysis evaluates whether higher governance maturity is associated with more complete and appropriately prioritized risk recognition.

3. Review of Literature

3.1 Artificial Intelligence and the Changing Boundary of Corporate Governance

The corporate-governance literature has historically treated information technology as an important but sometimes underdeveloped area of board oversight. Earlier work on IT governance argued that significant organizational dependence on information systems requires board-level participation because

technology decisions can affect strategy, internal control, regulatory compliance, and organizational value. Research on enterprise governance of information technology further developed structures through which boards can align technology with organizational objectives and monitor whether technology creates expected value while remaining appropriately controlled.

This argument becomes stronger when artificial intelligence influences decision processes rather than merely supporting infrastructure. Hilb proposes that AI can affect board activities through assisted, augmented, and potentially more autonomous forms of governance, while emphasizing that corporate governance must integrate business desirability, technological feasibility, and societal responsibility. Hickman and Petrin similarly show that trustworthy AI principles have implications for corporate leadership and intra-corporate oversight, particularly in relation to human intervention, technical robustness, privacy, and responsibility. The literature therefore supports viewing AI oversight as part of mainstream corporate governance rather than as an isolated IT-management issue.

3.2 Foundation Models, Generative Capability, and Organizational Risk

The technical literature explains why generative systems create distinctive governance challenges. Brown and colleagues demonstrated that large language models can perform many tasks from instructions or limited examples without conventional task-specific retraining. This adaptability increases potential business usefulness but also complicates risk classification because the same general-purpose system can be used for activities ranging from low-risk drafting to consequential financial, legal, or strategic analysis.

Bommasani and colleagues describe foundation models as systems trained broadly and adapted to many downstream tasks, emphasizing that their centrality creates both leverage and systemic risk because limitations in a foundational model can propagate across applications. Bender and colleagues add concerns regarding training-data scale, documentation, environmental effects, embedded biases, and inappropriate interpretation of generated language. These findings are directly relevant to boards because organizational risk cannot be assessed solely by asking whether a model is technically advanced. Governance must consider where the model is used, which information it receives, how outputs are reviewed, and what consequences follow from errors.

3.3 Accountability, Explainability, and Human Responsibility

AI governance literature repeatedly converges around accountability, transparency, fairness, privacy, and responsibility. Jobin, Ienca, and Vayena's mapping of international AI ethics guidelines identified considerable convergence around transparency, justice and fairness, non-maleficence, responsibility, and privacy, while also noting variation in how organizations translate those principles into practice. The European trustworthy-AI framework similarly emphasizes human agency, technical robustness, privacy and data governance, transparency, fairness, societal considerations, and accountability.

Accountability requires more than publishing technical documentation. Kroll and colleagues argue that automated decision systems require mechanisms capable of verifying whether computational processes satisfy relevant standards even where complete algorithmic transparency is impractical. NIST's explainability framework likewise stresses that explanations should provide reasons or evidence, be meaningful to relevant users, reflect the system's actual process, and respect appropriate knowledge

limits. For boards, these insights imply that oversight information should be decision-relevant rather than excessively technical. Directors require enough information to understand material exposures, challenge management assumptions, and determine whether accountability and control are credible.

4. Research Methodology

4.1 Research Design and Synthetic Governance Environment

The study adopts a quantitative simulation-based methodological design. No confidential board minutes, director assessments, enterprise AI inventories, vendor contracts, incident logs, prompt records, or model-evaluation datasets were provided. The study therefore does not represent a completed empirical examination of real corporations.

Seventy-two synthetic board-governance profiles are constructed and distributed equally across four oversight-maturity conditions. Each synthetic board is evaluated against six organizational Generative Artificial Intelligence scenarios: board-information summarization, management-report drafting, financial commentary generation, internal software-code generation, customer-communication assistance, and due-diligence document analysis. The resulting design contains 432 board-scenario assessments.

Table 1: Board-Level Dimensions Used in the Generative AI Oversight Model

Oversight Dimension	Representative Governance Evidence	Board-Level Question	Primary Governance Purpose
Strategic authorization	Approved AI principles and risk appetite	Has the board defined acceptable strategic boundaries?	Connects AI adoption with strategy and risk
Use-case visibility	Material AI inventory and risk classification	Does the board know where consequential GenAI is being used?	Reduces unmanaged or hidden adoption
Data and IP governance	Confidentiality, retention, licensing and data-use controls	Are information and intellectual-property exposures governed?	Protects corporate and stakeholder information
Model-risk control	Evaluation, testing, limitations and human review	Has management established controls proportionate to the use case?	Reduces inappropriate reliance on generated output
Human accountability	Named executive and business ownership	Is a responsible human owner identifiable for consequential use?	Prevents responsibility diffusion
Monitoring and escalation	Metrics, incident triggers, reporting and assurance	Are material failures detected and escalated to the appropriate level?	Supports continuing board oversight

Source: Author-developed simulation framework informed by corporate-governance, enterprise-risk, trustworthy-AI, and algorithmic-accountability literature.

The scenarios intentionally vary in consequence. Drafting an internal brainstorming note is treated differently from generating information incorporated into financial reporting or customer-facing communication. This risk-tiered design reflects the proposition that board oversight should be proportionate to organizational consequence rather than uniformly intensive across every use of generative technology.

4.2 Construction of the Board Generative AI Oversight Maturity Index

The Board Generative AI Oversight Maturity Index (BGOMI) combines six normalized dimensions:

[BGOMI_i = w_sS_i+w_uU_i+w_dD_i+w_mM_i+w_hH_i+w_eE_i]

where:

(S_i) = strategic authorization score; (U_i) = organizational use-case visibility; (D_i) = data and intellectual-property governance; (M_i) = model-risk control; (H_i) = human accountability; (E_i) = monitoring and escalation readiness.

For the baseline simulation, each dimension receives an equal weight:

[w_s=w_u=w_d=w_m=w_h=w_e=\frac{1}{6}]

with:

[\sum_{j=1}^{6}w_j=1]

The index ranges from 0 to 1. Equal weighting is used to avoid creating unsupported assumptions regarding the universal superiority of one governance dimension. In practical implementations, boards could assign higher weight to particular areas where organizational exposure is unusually high, such as confidential-data governance within financial institutions or intellectual-property protection in research-intensive enterprises.

The four synthetic maturity categories are defined as ad hoc GenAI use, policy-based governance, board-integrated oversight, and assured and adaptive oversight. These categories reflect increasing integration of generative-AI governance with enterprise risk, internal control, strategic planning, assurance, and incident management.

4.3 Generative AI Risk Recognition Score

The dependent analytical measure is the Generative AI Risk Recognition Score (GARRS). Each synthetic board receives points for recognizing and appropriately prioritizing six classes of risk: unreliable generated content, confidential-data exposure, bias or inappropriate content, intellectual-property risk, cybersecurity or malicious use, and weak human accountability.

The normalized score is calculated as:

[GARRS_i=\frac{\sum_{k=1}^{6} r_{ik}}{R_{max}}\times100]

where (r_{ik}) represents the points awarded to board (i) for risk domain (k), and (R_{max}) represents the maximum obtainable score.

Recognition does not require directors to prescribe technical mitigations. A board receives stronger performance where it identifies that a risk is material, requests appropriate management

evidence, clarifies ownership, and requires escalation or assurance proportionate to the consequence. This design preserves the governance-management boundary that underpins the study.

5. Analysis

5.1 Differences Across Oversight Maturity Conditions

The simulation indicates substantial differences between having an AI policy and possessing an effective oversight system. Synthetic organizations in the ad hoc category allow departments or employees to adopt generative tools independently, with incomplete visibility regarding data entered into models and limited board reporting. Boards in this condition can recognize obvious reputational concerns but frequently overlook third-party dependence, data retention, model limitations, and responsibility gaps.

Policy-based organizations perform better because acceptable-use rules and basic approval requirements exist. Nevertheless, several simulated boards receive aggregate information about AI adoption without a sufficiently clear connection between individual high-impact applications and the controls governing them. The analytical distinction is important: policy establishes expected behavior, whereas oversight requires evidence showing whether material use is actually occurring within those expectations.

Board-integrated organizations connect significant Generative Artificial Intelligence applications with enterprise-risk reporting, named executive ownership, use-case classification, and periodic board or committee review. The highest-maturity category adds independent testing or assurance, incident thresholds, model-change monitoring, and adaptive review when business conditions or model capabilities change.

5.2 Comparative Governance and Risk-Recognition Performance

Table 2: Simulated Board Oversight Maturity and Generative AI Risk Recognition

Oversight Condition	Mean BGOMI	Material Use-Case Visibility	Human Accountability Coverage	Escalation Readiness	Mean GARRS
Ad hoc GenAI use	0.22	41%	49%	44%	48
Policy-based governance	0.44	67%	69%	63%	64
Board-integrated oversight	0.70	86%	88%	81%	79
Assured and adaptive oversight	0.89	96%	95%	94%	90

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

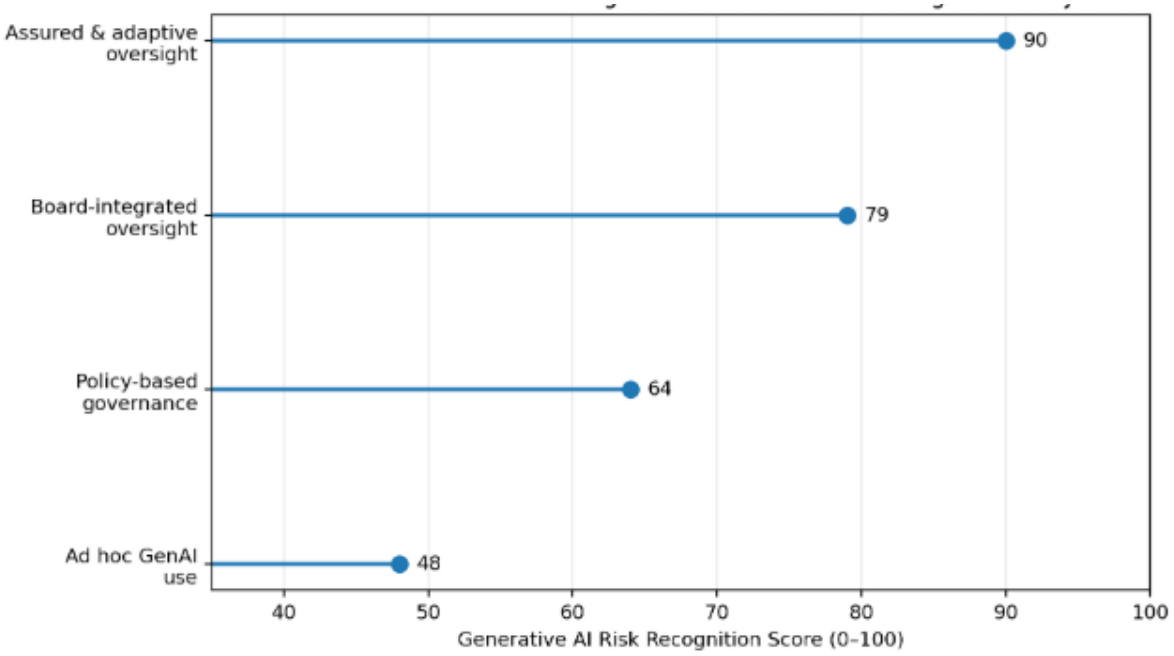
Note: All observations are simulated solely for methodological demonstration and do not represent measurements from real boards or companies.

The simulated results show that risk-recognition performance improves as generative-AI governance becomes more integrated with established corporate-governance processes. The largest improvement occurs between policy-based governance and board-integrated oversight. This suggests that written principles become substantially more useful when they are connected with ownership, risk reporting, use-case inventories, and escalation mechanisms.

The highest-maturity category does not achieve a perfect score. This is intentional because Generative Artificial Intelligence remains difficult to govern through static controls. New use cases can emerge, third-party models can change, employees can adapt systems to unexpected tasks, and previously acceptable applications can become more consequential as organizational dependence increases.

5.3 Board Risk Recognition Across Governance Maturity

Graph 1:Simulated Board Risk Recognition Across Generative AI Oversight Maturity



The graph illustrates progressive improvement in simulated risk recognition across the four oversight conditions. The mean Generative AI Risk Recognition Score increases from 48 under ad hoc adoption to 64 under policy-based governance, 79 under board-integrated oversight, and 90 under assured and adaptive oversight.

The pattern suggests that formal policies alone provide only partial governance value. Recognition improves most strongly when boards obtain reliable information about actual high-impact uses, responsible executives, underlying control architecture, and incidents requiring escalation.

Key Finding: Effective board oversight is associated in the simulation with a transition from knowing that Generative AI is being used to knowing where material use occurs, who is accountable, which risks are accepted, what controls exist, and how significant failures reach the board.

6. Discussion

6.1 The Board's Role Is Governance, Not Prompt-Level Management

The first implication concerns the appropriate boundary of director involvement. Generative AI is technically complex and rapidly changing, but this does not mean directors should approve specific prompts, model temperatures, retrieval configurations, or routine employee applications. Such activities belong to management and technical specialists.

Board responsibility becomes relevant where generative technology materially affects organizational strategy, risk, reporting, stakeholder treatment, or corporate assets. This position is consistent with enterprise-risk principles emphasizing board understanding of risk philosophy, risk appetite, significant exposures, and management's responses. It also aligns with research on digital governance showing that boards require meaningful technology-governance structures without attempting to perform operational IT functions themselves.

The board should therefore ask governance questions rather than engineering questions. Directors need to know whether management can identify material use cases, whether sensitive information can enter external models, whether high-consequence outputs receive human verification, whether third-party dependencies have been assessed, and whether incident reporting reaches an appropriate governance level.

6.2 Human Accountability Must Remain Visible

A second implication is that organizations should resist responsibility diffusion. Generative systems can create an appealing but problematic explanation for poor decisions: “the AI produced it.” Such language obscures the fact that humans decide whether a system may be deployed, which information it may process, how outputs are interpreted, and whether recommendations are acted upon.

Algorithmic-accountability research demonstrates that computational complexity does not remove the possibility or necessity of governance mechanisms. Trustworthy-AI guidance similarly treats accountability and auditability as essential alongside transparency and robustness. For board oversight, the practical consequence is that every material application should have identifiable business ownership even where the underlying model is supplied by an external technology vendor.

Human accountability also requires meaningful review. A nominal human approval step offers limited protection if reviewers routinely accept model output without sufficient time, expertise, or supporting evidence. Boards should therefore focus not only on whether “human oversight” exists but whether management has designed conditions under which humans can realistically detect and challenge significant model errors.

6.3 Oversight Must Become Adaptive Rather Than Periodic

The third implication is that generative-AI oversight cannot be based exclusively on annual technology reviews. Foundation-model research emphasizes the broad adaptability of general-purpose models and

the difficulties created when the same underlying technology supports many downstream applications. This characteristic means organizational risk can change even without formal acquisition of a new system.

A department may begin by using a model to rewrite internal text and later rely on the same tool for customer communication, contract analysis, or financial interpretation. The technology may remain identical while the organizational consequence changes materially. Governance processes therefore need trigger-based reassessment when data sensitivity, decision consequence, model dependence, user population, or external exposure changes.

Adaptive oversight should also incorporate assurance information. Boards need concise indicators capable of showing whether high-risk use cases have been tested, whether significant overrides or incidents are increasing, whether employees are bypassing approved systems, and whether changes in third-party models have altered organizational exposure. This reporting should be designed around governance decisions rather than overwhelming directors with technical metrics.

7. Conclusion

Generative Artificial Intelligence introduces important strategic opportunities, but its accessibility, adaptability, and general-purpose character also create governance challenges that differ from conventional enterprise technology. Organizational use can expand before boards possess a reliable picture of where models are being used, which information they process, how their outputs influence decisions, and which individuals remain responsible for consequential outcomes. Board oversight therefore needs to evolve alongside adoption.

This study proposes the Board Generative AI Oversight Maturity Index as a structured way to evaluate six governance dimensions: strategic authorization, use-case visibility, data and intellectual-property governance, model-risk control, human accountability, and monitoring and escalation readiness. A complementary Generative AI Risk Recognition Score evaluates whether boards can identify material weaknesses across different organizational use scenarios. Within the synthetic study environment, risk-recognition performance increases from 48 points under ad hoc adoption to 90 points under assured and adaptive oversight. These values illustrate the framework's internal logic and should not be treated as observed corporate benchmarks.

The study's broader governance position is that effective oversight lies between two extremes. Passive boards cannot assume that management or technology vendors will automatically identify every material risk. At the same time, directors should not become operational AI administrators. Their responsibility is to ensure that organizational objectives, risk appetite, accountability, controls, and assurance mechanisms remain coherent as generative systems become more deeply embedded in business processes. Material applications should have identifiable owners, proportionate control requirements, clear human-review expectations, and escalation pathways when significant failures occur.

The principal limitation is the simulation-based research design. Future empirical studies should test the proposed framework using authenticated board charters, committee materials, director technology expertise, enterprise AI inventories, risk registers, policy exceptions, internal-audit findings, AI incident records, and organizational performance outcomes. Research should also examine whether board digital competence, committee structure, industry regulation, firm complexity, technology

dependence, and assurance arrangements moderate the relationship between oversight maturity and AI-related outcomes. Board oversight of Generative Artificial Intelligence should ultimately be treated as an evolving component of corporate governance: sufficiently strategic to remain at board level, sufficiently technical to require specialist management support, and sufficiently consequential to demand clear human accountability.

References

1. Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in the military: A guide to the ethics of AI. *Philosophy & Technology, 32*, 1–15.
2. Hilb, M. (2020). Toward artificial governance? The role of artificial intelligence in shaping the future of corporate governance. *Journal of Management and Governance, 24*, 851–870.
3. Martin, K. (2019). Ethical implications and accountability of algorithms. *Journal of Business Ethics, 160*, 835–850.
4. Martin, K. E., & Freeman, R. E. (2004). Some problems with employee monitoring. *Journal of Business Ethics, 50*, 267–279.
5. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society, 3*(2), 1–21.
6. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., et al. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines, 28*, 689–707.
7. Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence, 1*, 389–399.
8. Rai, A. (2020). Explainable AI: From black box to glass box. *Journal of the Academy of Marketing Science, 48*, 137–141.
9. Jarrahi, M. H. (2018). Artificial intelligence and the future of work: Human–AI symbiosis in organizational decision making. *Business Horizons, 61*(4), 577–586.
10. Shrestha, Y. R., Ben-Menahem, S. M., & von Krogh, G. (2019). Organizational decision-making structures in the age of artificial intelligence. *California Management Review, 61*(4), 66–83.
11. Raisch, S., & Krakowski, S. (2021). Artificial intelligence and management: The automation–augmentation paradox. *Academy of Management Review, 46*(1), 192–210.
12. Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California Management Review, 61*(4), 5–14.
13. Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., et al. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management, 57*, 101994.
14. Wirtz, J., Weyerer, J. C., & Geyer, C. (2019). Artificial intelligence and the public sector—Applications and challenges. *International Journal of Public Administration, 42*(7), 596–615.
15. Aoki, K. (2020). An empirical study of board-level governance of artificial intelligence. *Corporate Governance: The International Journal of Business in Society, 20*, 1–15.

16. Katyal, V., Liepold, C., Iyengar, S., Mittal, N., & Saif, I. (2020). Artificial intelligence and ethics: An emerging area of board oversight responsibility. *Harvard Law School Forum on Corporate Governance*.
17. McKinsey & Company. (2019). *Notes from the AI frontier: Tackling Europe's gap in digital and AI*. McKinsey Global Institute.
18. National Association of Corporate Directors. (2020). *Artificial Intelligence: An Emerging Oversight Responsibility for Boards*. NACD.
19. Cunningham, L. A., Maskin, A., Carlson, J. B., Castelluccio, J. A., Noreuil, A. J., Peterson, B. L., & de Bernier, P. C. (2023). Generative artificial intelligence and corporate boards: Cautions and considerations. *Mayer Brown Legal Insights*.
20. Society for Corporate Governance. (2023). *Board Practices: Artificial Intelligence*. Society for Corporate Governance.