

Artificial Intelligence (Ai) in Corporate Governance: Board Accountability and Directors' Duties in India and Abroad

Riddhika Tiwari^{1*}, Prof. (Dr.) Aradhana Parmar²

¹ Research Scholar, Faculty of Law, Maharishi Arvind University, Jaipur, Rajasthan, India

riddhikatiwari7@gmail.com

² Supervisor, Faculty of Law, Maharishi Arvind University, Jaipur, Rajasthan, India

Abstract: Artificial intelligence increasingly shapes information and recommendations reaching corporate boards. It can strengthen forecasting, detect irregularities, and improve organizational responsiveness, but it can also conceal unreliable assumptions, reproduce discrimination, and weaken meaningful human scrutiny. This article examines how directors' duties apply when companies adopt AI, with particular attention to India and comparative developments in the United Kingdom, United States, and European Union. Using doctrinal and comparative analysis, it argues that AI changes the practical demands of oversight without eliminating human responsibility. Existing duties provide an important foundation, although their application requires attention to organizational context, foreseeable risks, and the director's role. The article proposes proportionate governance arrangements covering system approval, vendor scrutiny, monitoring, incident escalation, and correction. Its central conclusion is that responsible adoption depends on directors' ability to question evidence and act on warning signs, rather than treating automated recommendations as substitutes for judgment.

Keywords: Artificial Intelligence, Corporate Governance, Board Accountability, Directors' Duties, Fiduciary Responsibility, Algorithmic Oversight, Responsible Innovation, Comparative Corporate Law

INTRODUCTION

A board considering an acquisition may receive an AI-generated assessment that appears comprehensive and precise. It may identify financial opportunities, summarize legal risks, and recommend a particular course. Yet the report may contain outdated information or assumptions that favour expansion. The directors' responsibility begins with recognizing that an impressive presentation does not establish a reliable basis for action. They must understand what the assessment can support, what remains uncertain, and when further advice is necessary.

AI creates a distinctive governance problem because its influence often extends beyond visible boardroom tools. Recruitment systems shape the workforce, pricing models affect customers, and automated fraud detection can restrict access to services. Decisions taken below board level may therefore generate strategic, legal, and reputational consequences. Directors cannot

supervise every output, but they should ensure that material risks are identified and communicated through workable reporting arrangements.

This article asks how established duties should guide that supervision. It examines legislation, judicial decisions, and policy instruments, distinguishing enforceable obligations from voluntary guidance and proposed reforms. The discussion advances a proportionate approach: the intensity of oversight should reflect the significance of the application, the potential harm, and the organisation's capacity to detect and correct failure.

Historical Background

Corporate governance emerged from a practical difficulty that remains recognizable today: people controlling a business may possess information and pursue interests different from those of its owners. Berle and Means (1932) examined the separation between ownership and control in large corporations. Their work highlighted the importance of institutional arrangements capable of making managerial power answerable. AI does not replace this problem. It introduces another source of informational dependence within it. Directors may now rely on managers who rely on technical teams and external suppliers, creating a longer chain between corporate authority and the evidence supporting its exercise.

The development of directors' duties reflected attempts to discipline corporate power without preventing legitimate commercial judgment. Boards needed freedom to pursue opportunities, but that freedom required standards of loyalty, care, and responsibility. Over time, governance came to include the quality of information systems and internal controls through which directors understood the business. This historical development matters because AI is sometimes presented as an entirely new legal territory. Although its technical characteristics are distinctive, the underlying questions concerning delegation, supervision, conflicts, and informed judgment have substantial roots in corporate law and organizational practice across different legal traditions.

The intellectual history of AI developed along a different path. Turing (1950) explored whether machines could display behaviour associated with intelligence, helping establish questions that continue to shape technological debate. McCarthy and colleagues (1955) subsequently proposed the Dartmouth research project, bringing artificial intelligence into a defined research agenda. These early contributions did not establish modern corporate

applications, but they encouraged the possibility that machines could perform activities associated with human reasoning. Their significance for governance lies in a gradual change in expectations: computers could increasingly become participants in producing recommendations, rather than merely instruments for storing information.

Early business computing largely supported accounting, payroll, inventory, and other structured processes. Its governance implications concerned data accuracy, access controls, system reliability, and the continuity of operations. As analytical tools became more sophisticated, companies increasingly used statistical models to support forecasting, credit assessment, and resource allocation. Decision authority formally remained with individuals, yet the information shaping their choices became more technologically mediated. This experience established a lesson relevant to contemporary AI: adopting a system does not remove the need to understand its purpose and limitations. Organizational convenience can otherwise encourage reliance beyond the conditions for which a tool was developed.

Agency theory sharpened the explanation of these organizational difficulties. Jensen and Meckling (1976) examined relationships in which one party acts on behalf of another and explored the associated costs of monitoring and divergent incentives. Applied cautiously to AI governance, this perspective reveals several overlapping relationships. Shareholders depend on directors, directors depend on executives, and executives depend on suppliers whose commercial interests may favour rapid deployment. Technical assurances can therefore reflect incentives as well as expertise. Effective governance requires a setting in which inconvenient findings can travel upwards, rather than being filtered out because they challenge an approved investment.

Developments in American oversight jurisprudence further connected board responsibility with information and reporting arrangements. In *re Caremark International Inc. Derivative Litigation* (1996) addressed directors' oversight responsibilities within the demanding standards governing such claims. The case did not impose liability whenever compliance failed. Its wider importance lies in recognizing that corporate supervision requires a good-faith effort to establish appropriate information systems. For AI, the analogy is institutional rather than technological. A board may need reliable channels for discovering serious problems even though directors cannot personally inspect every model or operational decision. The comparison does not convert every technical defect into fiduciary misconduct.

Legislative developments also made expectations more explicit. The United Kingdom's Companies Act 2006 articulated duties concerning independent judgment and reasonable care, skill, and diligence. India's Companies Act, 2013 similarly codified important directors' duties, including care, diligence, and independent judgment under section 166. These provisions were not written as detailed AI regulations. Nevertheless, they supply standards through which later technologies can be assessed. The historical lesson is that general duties can remain relevant while their practical application evolves. What constitutes reasonable inquiry may change as a technology becomes more influential, better understood, and capable of affecting corporate interests.

The growth of data-driven business widened governance concerns beyond financial performance. Personal information became central to advertising, recruitment, lending, and customer profiling. GDPR provided an influential framework for personal-data protection and addressed certain solely automated decisions producing legal or similarly significant effects (European Parliament & Council of the European Union, 2016). This development connected technology governance with the position of affected individuals. For boards, it demonstrated that efficiency could not be evaluated independently of lawful processing and procedural safeguards. Data practices became matters capable of affecting organizational legitimacy, trust, and exposure to legal and regulatory consequences.

India's policy trajectory subsequently linked AI development with inclusion and responsibility. The National Strategy for Artificial Intelligence identified opportunities for social and economic benefit, while NITI Aayog's responsible AI documents examined principles and their operationalization (NITI Aayog, 2018, 2021a, 2021b). Internationally, the OECD's 2019 recommendation and UNESCO's 2021 recommendation advanced expectations concerning accountability and human-centered development. These instruments differ from company legislation in legal form and enforcement. Their historical contribution was to provide a shared vocabulary through which governments and businesses could discuss fairness, transparency, safety, and oversight without assuming that one institutional model would suit every application.

Generative AI has brought these historical strands into closer contact. Systems now produce fluent narratives, draft reports, and summarize material for decision-makers, increasing the possibility that presentation will be mistaken for verification. NIST's framework, the

European Union's AI Act, the Council of Europe's convention, and India's 2025 guidelines reflect different responses to this expanding influence (Council of Europe, 2024; MeitY, 2025; Tabassi, 2023). Across this history, the continuing challenge is organizational: preserving a clear relationship between authority, evidence, and responsibility when important reasoning processes become less visible to those expected to supervise them.

This continuity explains why effective reform must connect technical safeguards with established institutions, rather than assume that purchasing advanced technology also purchases sound judgment or organizational integrity.

Research Approach

The analysis uses doctrinal comparison to examine how established legal duties interact with contemporary AI governance instruments. Legislation and judicial decisions provide the legal foundation, while policy frameworks assist in identifying practical responses. The comparison does not assume that rules can be transferred unchanged between jurisdictions. Differences in corporate structure, enforcement, and legal tradition affect their operation. The article therefore separates descriptive statements about existing law from recommendations concerning governance practice. It does not report original interviews, survey findings, or measured corporate outcomes. Its contribution is an interpretive framework for asking what responsible board conduct should involve when material business activities depend on AI.

Directors' Duties and the Indian Legal Framework

Section 166 of the Companies Act, 2013 provides the principal starting point. Directors must act in good faith within the statutory framework, exercise due and reasonable care, skill, and diligence, and exercise independent judgment. Applied to AI, these duties support an obligation to inquire into material risks before accepting consequential recommendations. This is an interpretation of general duties, rather than an assertion that the section expressly mandates a particular AI committee or technical audit.

Independent judgment does not require directors to disregard specialist advice. It requires them to assess advice rather than surrender their decision-making role. A director approving an AI-supported investment need not reproduce the model's calculations, but should understand the recommendation's purpose, significant assumptions, and limitations. Where the consequences are substantial, obtaining independent validation may be reasonable. The relevant standard

depends on the circumstances, rather than a universal requirement that every system undergoes identical scrutiny.

The statutory duty to avoid conflicts also matters when directors have interests in AI suppliers or related enterprises. Procurement decisions should follow applicable disclosure and approval requirements. Commercial enthusiasm must not obscure a relationship capable of compromising objective assessment. Similarly, the company's interests cannot be assessed solely through a vendor's projected efficiency gains. Directors should examine foreseeable effects on customers, employees, operational resilience, and legal compliance within the applicable statutory framework.

For listed companies, SEBI's governance framework provides an additional setting for risk supervision (SEBI, 2015). AI should be integrated into appropriate existing responsibilities, including relevant audit, risk, and internal-control processes. Personal-data uses also require attention to the Digital Personal Data Protection Act, 2023 and applicable commencement arrangements. India's 2025 AI Governance Guidelines strengthen the policy case for responsible adoption, but do not themselves replace company law or establish a comprehensive code of directors' civil liability (MeitY, 2025).

INTERNATIONAL PERSPECTIVES

United Kingdom

Sections 173 and 174 of the Companies Act 2006 require independent judgment and reasonable care, skill, and diligence. Section 174 combines an objective standard with attention to the director's actual knowledge, skill, and experience. In an AI setting, this supports proportionate inquiry informed by the director's position and expertise. Technical specialization can therefore affect expectations, while other directors remain responsible for asking questions appropriate to their roles. These provisions do not guarantee that a properly considered business decision will succeed.

United States

Delaware oversight law offers a comparison concerning serious reporting failures. In *Marchand v. Barnhill* (2019), the Delaware Supreme Court reversed dismissal of a claim alleging the absence of board-level monitoring of food safety in a company whose business

depended on that issue. The case concerned food safety, not AI, and did not establish final liability. Its relevance is analogical: when a risk is central to the business, directors should consider whether board-level information arrangements meaningfully address it. American oversight claims remain subject to demanding legal thresholds.

NIST's voluntary framework provides practical support through its governance, mapping, measurement, and management functions (Tabassi, 2023). Boards can use it to organize questions and evaluate reporting. Compliance with a voluntary framework is neither an automatic defence nor proof that every legal obligation has been satisfied.

European Union

The AI Act distinguishes obligations by risk and by organizational role, including responsibilities relevant to providers and deployers of specified systems. Its structure illustrates why boards must identify what the company actually does within the AI lifecycle. A company developing a system may face obligations different from those of a business deploying a purchased application (European Parliament & Council of the European Union, 2024).

GDPR separately governs personal-data processing and certain solely automated decisions. Neither framework makes all automated decision-making unlawful or all directors personally liable. Their combined governance significance lies in requiring organizations to connect system design and operation with applicable legal responsibilities, rather than considering compliance only after deployment.

International Principles

The OECD recommendation, UNESCO recommendation, and Council of Europe convention connect AI governance with accountability and human rights. Their legal forms differ: recommendations are not interchangeable with treaty obligations, and treaty effects depend on participation and implementation. They nevertheless support a comparative insight: internal accountability should include attention to affected people, alongside operational and financial performance.

Contemporary Governance Challenges

Generative AI can produce plausible statements unsupported by reliable evidence. When such material enters board papers, directors may make decisions on an inaccurate account of law, finance, or market conditions. Important factual and legal claims therefore require verification against authoritative sources. The challenge is heightened when an AI-generated summary removes qualifications that were present in the original material.

Vendor dependence creates another difficulty. A company may purchase an application without sufficient access to testing results, update information, or incident records. Responsibility then becomes fragmented between procurement, legal, technology, and business teams. Boards should ensure that someone can assemble these separate perspectives and identify risks that no single department sees completely.

More autonomous systems also raise questions about authority. An AI agent able to communicate externally, initiate transactions, or change operational settings can generate consequences before a person reviews them. Approval limits, access permissions, and reliable interruption mechanisms should match that authority. Monitoring only whether the system remains available is insufficient when its actions can affect contractual commitments or third parties.

Bias and workforce effects require equal attention. An efficient recruitment model may systematically overlook suitable applicants, while workplace monitoring can undermine trust if employees cannot question inaccurate assessments. These possibilities require context-sensitive testing and complaint procedures. Governance should examine how a system behaves in actual use, rather than relying exclusively on performance demonstrated during procurement.

Accountability and Personal Liability

Accountability includes explaining decisions, correcting weaknesses, and accepting scrutiny. Personal legal liability requires the elements of a particular claim to be established. Keeping these concepts distinct prevents two errors: assuming that every harmful output proves misconduct, and assuming that technical complexity excuses all inquiry. An adverse result may occur despite reasonable precautions. Conversely, a profitable system may still be

governed irresponsibly if serious legal warnings are ignored. Assessment should examine the process and the applicable duty, rather than infer legality from commercial success or failure.

The distinction also matters when responsibilities are allocated among committees and executives. Delegation can improve supervision by matching tasks with expertise, but the board needs sufficient information to evaluate whether that arrangement works. An AI specialist on the board should strengthen collective understanding rather than become the only person expected to engage with technological risk. Independent directors require usable reporting and opportunities to challenge management. Their liability must still be assessed under the statutory conditions applicable to their role. Governance design should therefore make responsibility identifiable without pretending that every participant controls every stage of development and deployment.

A Proportionate Framework for Board Accountability

The board should first ensure that the company knows where consequential AI is used. An inventory should distinguish routine assistance from systems influencing significant rights, resources, or commitments. Each important application should have an identified executive owner, a defined purpose, and a route for escalating concerns. This framework is a governance recommendation, not a claim that every company is presently subject to an identical statutory checklist.

Before approval, management should explain expected benefits, affected groups, major limitations, and available alternatives. Vendor contracts should address access to relevant information, security, updates, incident cooperation, and termination. A board should question whether the company can supervise what it purchases. Where opacity prevents proportionate assurance, restricting the proposed use may be more reasonable than relying on broad contractual promises.

After deployment, reporting should identify material errors, complaints, unusual patterns, and changes in performance. Review should respond to changes in the model, data, or operating environment. Serious incidents require clear authority to pause a system, investigate, and correct decisions where appropriate. Human review becomes meaningful only when the reviewer has adequate information, time, competence, and power to alter the result.

Board minutes should record substantive questions, significant uncertainty, advice received, and reasons for approval. Documentation should reflect deliberation rather than merely record that a presentation occurred. Director training should build enough understanding to recognize when specialist help is needed. Smaller companies can adapt these arrangements through simpler approval records and shared expertise, provided the response remains proportionate to the risks involved.

CONCLUSION

AI changes how corporate decisions are prepared and implemented, but it does not dissolve the institutional responsibilities attached to corporate authority. Indian company law and comparative frameworks provide useful foundations for oversight, although their legal forms and liability standards differ. Directors should be assessed through their applicable duties, conduct, and circumstances, rather than the mere occurrence of an adverse output. Responsible governance requires informed approval, credible reporting, and timely intervention. Innovation becomes more sustainable when directors can explain why a system was adopted, how material risks were examined, and what the company will do when its assumptions prove wrong.

FUTURE SCOPE

Future research should examine actual board practices rather than infer effectiveness from published policies. Interviews, incident studies, and analysis of approval records could reveal whether directors receive information capable of changing decisions. Comparative work should investigate how company size, ownership, and sector influence oversight. Further inquiry is needed into autonomous agents, director competence, insurance, and the allocation of responsibility between companies and suppliers. Indian regulators could develop coordinated, sector-sensitive guidance while avoiding unnecessary duplication. The most useful reforms will be those that improve the organisation's capacity to detect problems, listen to affected people, and act before harm becomes widespread. Research should also distinguish between policies that exist on paper and practices that give directors timely evidence and affected individuals a realistic opportunity to obtain explanation, review, and correction.

References

1. Berle, A. A., Jr., & Means, G. C. (1932). *The modern corporation and private property*. Macmillan.
2. Turing, A. M. (1950). Computing machinery and intelligence. *Mind*, 59(236), 433–460. <https://doi.org/10.1093/mind/LIX.236.433>
3. McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (1955). *A proposal for the Dartmouth summer research project on artificial intelligence*. Dartmouth College. <http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html>
4. Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360. [https://doi.org/10.1016/0304-405X\(76\)90026-X](https://doi.org/10.1016/0304-405X(76)90026-X)
5. In re Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996).
6. Companies Act 2006, c. 46 (UK). (2006). <https://www.legislation.gov.uk/ukpga/2006/46/contents>
7. Companies Act, No. 18 of 2013 (India). (2013). Government of India.
8. Securities and Exchange Board of India. (2015). *Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015*. <https://www.sebi.gov.in/legal/regulations.html>
9. European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
10. NITI Aayog. (2018). *National strategy for artificial intelligence: #AIForAll*. Government of India.
11. Marchand v. Barnhill, 212 A.3d 805 (Del. 2019). <https://law.justia.com/cases/delaware/supreme-court/2019/533-2018.html>

12. Organization for Economic Co-operation and Development. (2019). *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449; amended 2024). <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
13. NITI Aayog. (2021a). *Responsible AI #AIForAll: Approach document for India. Part 1—Principles for responsible AI*. Government of India. <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf>
14. NITI Aayog. (2021b). *Responsible AI #AIForAll: Approach document for India. Part 2—Operationalizing principles for responsible AI*. Government of India.
15. United Nations Educational, Scientific and Cultural Organization. (2021). *Recommendation on the ethics of artificial intelligence*. <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>
16. Digital Personal Data Protection Act, No. 22 of 2023 (India). (2023). Government of India.
17. 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>
18. Council of Europe. (2024). *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CETS No. 225). <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>
19. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, 2024/1689. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
20. Ministry of Electronics and Information Technology. (2025). *India AI governance guidelines*. Government of India. <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf>