ETHICAL AI AND CORPORATE GOVERNANCE: DESIGNING INTERNAL COMPLIANCE FOR RESPONSIBLE AI USE

- Plabanee Patnaik* & Sidhant Soin**

Abstract

The current legal and operational frameworks of corporate governance are significantly and structurally challenged by the use of fully autonomous and semi-autonomous Artificial Intelligence (AI) in business decision-making. The new risks that AI introduces, such as algorithmic bias, "black box" opacity, and the potential for systemic harm to occur at an unprecedented speed and scale, are not well addressed by traditional models, which are predicated on human agency and clear lines of accountability. According to this article, in order to address this new situation and ensure that its directors fulfil their fiduciary responsibilities, a company must completely restructure its internal compliance. This is not only a commendable concept, but it is also a moral and legal obligation. This article illustrates this point by segmenting it into three distinct components. Initially, it provides a concise, practical definition of "Responsible AI" that is applicable to both legal and business contexts. Secondly, it conducts a critical comparative analysis of the global regulatory landscape that is currently broken, examining the respective approaches of the European Union, the United States, and India. Third, it examines traditional concepts regarding corporate liability and fiduciary duty in the context of algorithms and demonstrates the necessity of a more rigorous application of these concepts. The article concludes with a set of guidelines for a novel approach to ensuring that all employees adhere to the rules. These regulations are predicated on four interconnected pillars: proactive AI Impact Assessments, top-down governance, robust audit trails, and a comprehensive corporate AI policy. This comprehensive framework provides businesses with a means to capitalise on the advantages of AI while simultaneously mitigating its significant risks, which are both ethical and legal.

* Advocate, Email: plabaneepatnaik11@gmail.com
** Advocate, Email: sidhantsoin@gmail.com

***Keywords**: AI, Governance, Ethical AI, Algorithmic Accountability, EU AI Act.*

INTRODUCTION

The contemporary corporation is founded on delegated authority and is managed by systems of human oversight and accountability.[1] The entire framework of corporate law, as evidenced by the significant case of *Salomon* v. *A. Salomon Co. Ltd.*[2], is based on this principle. The concept of a distinct legal entity that is managed by human agents has been the foundation.[3] This structure is fundamentally altered by Artificial Intelligence (AI).[4] The incorporation of fully automated and semi-automated systems for critical business operations, including credit-risk assessment, hiring, supply chain management, and high-frequency trading[4], introduces a novel form of agency to the corporate ecosystem. This system operates at a scale, speed, and level of complexity that renders it difficult for individuals to monitor. Consequently, a governance gap exists that current legal and compliance models were not designed to address.[5]

This discrepancy has tangible consequences. A company's reputation and finances can be significantly impacted by poorly managed AI, as evidenced by high-profile failures. Businesses are currently confronted with issues such as discriminatory algorithms[6], biassed loan-adjudication systems[7], and dangerously flawed self-driving cars[8], which are not hypothetical scenarios. The question of "who is responsible?" becomes extremely complex when an AI system causes harm. Is it the developer who authored the code, the vendor who

[1] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* 8 (PublicAffairs, New York, 2019).
[2] Salomon v. A. Salomon & Co. Ltd., [1897] AC 22 (HL).
[3] Lawrence B. Solum, "Legal Personhood for Artificial Intelligences" 70 *North Carolina Law Review* 1231 (1992).
[4] Donald MacKenzie, "How to Make Money in Microseconds" 21 *London Review of Books* 16 (2011).
[5] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 3 (Harvard University Press, Cambridge, 2015).
[6] Jeffrey Dastin, "Amazon scraps secret AI recruiting tool that showed bias against women" *Reuters*, Oct. 10, 2018, *available at*: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G (last visited on: 27.06.2025).
[7] Julia Angwin, *et.al.*, "The Secret Bias Hidden in Mortgage-Approval Algorithms" *The Markup*, Aug. 25, 2021, *available at*: https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms (last visited on June 27, 2025).
[8] Cade Metz, "Uber's Self-Driving Car Didn't Know Pedestrians Could Jaywalk" *The New York Times*, Nov. 6, 2019, *available at*: https://www.nytimes.com/2019/11/06/technology/uber-self-driving-car-arizona.html (last visited on: 27.06.2025).

supplied the system, the manager who implemented it,[9] or the board of directors who authorised its use without a comprehensive understanding of the potential hazards?

This article addresses the central challenge. It asserts that applying high-level ethical principles on a case-by-case basis is inadequate.[10] In order to survive the algorithmic era, organisations must establish a new, robust internal compliance architecture that is specifically designed to regulate AI. This is not merely a matter of being socially responsible or doing the right thing[11]; it is becoming an essential component of the fiduciary duties of care and oversight that directors are obligated to fulfil for the company.

The primary inquiry that this research aims to address is: *To what extent do current corporate governance frameworks and fiduciary obligations, which were designed for organisations that are managed by humans, effectively ensure the responsible development and utilisation of autonomous AI systems? In order to address this accountability gap, which internal compliance structures are legally mandated?*

To address this, the article emphasises that conventional corporate governance models, particularly the business judgement rule and the duty of oversight, are inadequate in addressing the distinctive risks associated with AI due to their reliance on assumptions regarding human cognition and decision-making. In order to fulfil their fiduciary obligations, corporate boards must establish a new, integrated compliance architecture in the era of AI. This architecture is composed of four primary components:

(1) Board-level technological proficiency and transparent accountability at the highest levels.
(2) Mandatory AI Impact Assessments (AIIAs) prior to deployment;
(3) The maintenance of comprehensive and auditable algorithmic records; and
(4) The development of a comprehensive, company-wide AI Policy.

This article comprises five sections.

[9] W.K.C. Guthrie, *A History of Greek Philosophy, Vol. 3: The Fifth-Century Enlightenment* 129 (Cambridge University Press, 1969).
[10] Luciano Floridi, "Translating Principles into Practices: A Diachronic and Syncronic Analysis of AI Ethics" 1 *Philosophy & Technology* 1-12 (2019).
[11] A. C. Fernando, *Corporate Governance: Principles, Policies and Practices* 42 (Pearson Education, New Delhi, 3rd edn., 2015).

- The Part II of the article will deconstruct the concept of "Responsible AI" from a vague ideal to a concrete, risk-based standard that businesses can employ to maintain compliance.
- Part III examines the necessity of reevaluating and applying conventional corporate law principles, such as the duty of care and the Caremark standard for oversight liability, to regulate AI systems.
- Part IV examines the regulatory environments of the European Union, the United States, and India, and it compares them in order to identify significant trends and legal pressures.
- The primary contribution of this work is illustrated in Part V, which provides a comprehensive plan for an integrated internal compliance framework.
- Ultimately, the article concludes with recommendations for modifications to the law and the practices of businesses.

It asserts that the most effective method of fostering genuine corporate responsibility in the algorithmic era is to develop proactive internal compliance systems.

HOW TO IMPLEMENT "RESPONSIBLE AI" IN CORPORATE GOVERNANCE

The terms "*ethical AI*" and "*responsible AI*" are frequently used interchangeably; however, it is crucial to distinguish between the two in order to ensure legal compliance and corporate governance.[12] In a legal and corporate context, responsibility refers to accountable, auditable, and risk-managed behaviour, while ethics are broad, normative principles.[13] The objective of a board of directors is not merely to contemplate ethics, but to establish a tangible framework for the *responsible* deployment of AI.[14] We can establish a practical definition of Responsible AI for corporate governance that is based on four primary, actionable principles: Fairness, Transparency, Accountability, and Security (FTAS) through the implementation of new regulations and the consensus of experts.

Fairness: The Obligation to Minimise Algorithmic Bias

[12] Virginia Dignum, *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way* (Springer, 2019).
[13] Aristotle, *Nicomachean Ethics*, Book II (W.D. Ross trans., Oxford University Press, 2009).
[14] Mireille Hildebrandt, "The Artificial Intelligence of Law. Who is the Master?", in Mireille Hildebrandt & Antoinette Rouvroy (eds.), *Law, Human Agency and Autonomic Computing* 115 (Routledge, 2011).

When an AI system consistently generates biassed results, it reinforces and frequently exacerbates biases that are already present in its training data, a phenomenon known as algorithmic bias occurs.[15] This is not a technical issue; rather, it is a significant governance challenge.[16] The company is at risk of legal and reputational damage under anti-discrimination laws if a loan adjudication system demonstrates racial bias[17] or an AI system used for hiring unfairly rejects qualified female candidates.[18] Consequently, before and *during* the deployment of an AI system, the principle of fairness necessitates the identification, measurement, and mitigation of these biases.[19] This includes ensuring that all individuals have equal opportunities, which is a critical component of human rights and anti-discrimination legislation, in addition to ensuring that the numbers are equal.[20]

The Necessity of Clear Explanations: Transparency

Many advanced AI systems, particularly those that employ deep learning, operate as "black boxes."[21] The internal decision-making logic of these systems is so intricate that even their creators are unable to decipher it. This lack of clarity is in direct opposition to the legal principles of due process and reasoned decision-making.[22] For instance, an AI that denies credit to an individual is unable to appeal or review the decision without understanding the rationale behind it[23]. Transparency, or "*explainability*," necessitates that AI systems provide explicit, human-comprehensible rationales for their outputs.[24] It is not always necessary to provide proprietary code; however, it is necessary to be able to articulate the primary factors and reasoning that resulted in a particular decision, particularly one that has significant legal or financial repercussions.

Determining Responsibility in an Autonomous System

[15] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* 21 (Crown, New York, 2016).
[16] Solon Barocas and Andrew D. Selbst, "Big Data's Disparate Impact" 104 *California Law Review* 671 (2016).
[17] *Supra* note 6.
[18] *Supra* note 7.
[19] The Equal Credit Opportunity Act, 15 U.S.C. sec. 1691-1691f (United States).
[20] The Constitution of India, art. 15.
[21] *Supra* note 5 at 107.
[22] *State* v. *Loomis*, 881 N.W.2d 749 (Wis. 2016).
[23] Danielle Keats Citron and Frank Pasquale, "The Scored Society: Due Process for Automated Predictions" 89 *Washington Law Review* 1 (2014).
[24] Bryce Goodman and Seth Flaxman, "European Union Regulations on Algorithmic Decision-Making and a 'Right to Explanation'" 38 *AI Magazine* 50 (2017).

Corporate governance's most critical component is accountability.[25] It implies that each action taken by a company must be accompanied by explicit lines of authority and responsibility. This is further complicated by the inclusion of autonomous agents in the decision-making process.[26] True accountability for AI requires that a specific individual or organisation be held accountable for any action taken by an AI system.[27] To achieve this, a governance framework that clearly defines roles and responsibilities for the entire AI lifecycle, from data collection and model training to deployment, monitoring, and decommissioning, is necessary. The AI system becomes a convenient scapegoat if this does not occur, which weakens the very concept of corporate liability and disseminates responsibility.[28]

Obligation to Prevent Emerging Security Threats

Safety is the final regulation. New vulnerabilities are generated by AI systems. Adversarial attacks can compromise them by subtly altering the input data, causing the system to make significant errors, or by corrupting the training data through poisoning.[29] It is the responsibility of a company that employs AI to ensure that its systems are robust and secure against these types of threats, a principle identified as "*secure by design*."[30] This is not merely a cybersecurity concern; it is also a critical component of risk management. The failure to safeguard the control system of an autonomous vehicle or a financial trading algorithm from a malicious attack is a severe violation of the duty of care.[31]

The vague concept of "Responsible AI" is transformed into a precise set of objectives for the operation of an organisation by these four concepts—Fairness, Transparency, Accountability,

[25] Robert C. Clark, *Corporate Law* 34 (Aspen Publishers, 1986).
[26] Samir Chopra & Laurence F. White, *A Legal Theory for Autonomous Artificial Agents* 77 (University of Michigan Press, 2011).
[27] Andrea Renda, *The 'Do-ocracy' of AI: Governance by Experimentation* 4 (Centre for European Policy Studies, 2019).
[28] Ryan Abbott, *The Reasonable Robot: Artificial Intelligence and the Law* 45 (Cambridge University Press, 2020).
[29] Ram Shankar Siva Kumar, *et.al.*, "Adversarial Machine Learning - Industry Perspectives", paper presented at AISec '18: Proceedings of the 11th ACM Workshop on Artificial Intelligence and Security (October 2018), *available at*: https://dl.acm.org/doi/10.1145/3270101.3270104 (last visited on: 27.06.2025).
[30] European Union Agency for Cybersecurity (ENISA), *Securing AI*, November 2020, *available at*: https://www.enisa.europa.eu/publications/securing-ai (last visited on: 27.06.2025).
[31] David C. Vladeck, "Machines without Principals: Liability Rules and Artificial Intelligence" 89 *Washington Law Review*117 (2014).

and Security. They provide a method for evaluating the effectiveness of a board and the adherence of a company to its regulations.

IN THE ERA OF ALGORITHMS, HOW CAN FIDUCIARY DUTIES BE INTERPRETED DIFFERENTLY?

Corporate fiduciary law is founded on two fundamental principles: loyalty and care. In the best interests of the corporation, directors must act as if they are a reasonably prudent individual.[32] The use of AI does not create new fiduciary duties; however, it significantly alters the way in which these duties are understood and applied.[33]

The Problem of Technological Competence and the Duty of Care

In the past, the duty of care mandated that directors must possess a comprehensive understanding of the technologies in use before making a business decision.[34] However, in the current era of AI, this definition of "*important information*" must also encompass a comprehensive understanding of the technologies. It is impossible for a board to make an informed decision when they approve the expenditure of millions on a core AI system without understanding its primary risks, such as its potential for bias or its "*black box*" operation.[35]

This raises the question of technological proficiency. Although directors are not required to be data scientists, courts may begin to perceive a complete and passive lack of knowledge about basic technology risks as a breach of the duty of care.[36] Directors are shielded from liability for honest errors in judgement by the business judgement rule; however, the decision must be made with sufficient knowledge.[37] A decision to employ a powerful, opaque AI system without conducting sufficient research into its potential risks is not merely a lapse in judgement; it is a failure of the process.[38] The business judgement rule may not be applicable

[32] The Companies Act, 2013 (Act 18 of 2013), sec. 166.
[33] Lynn A. Stout, "The Shareholder Value Myth" 33 *Stetson Law Review* 116 (2003).
[34] *Aronson* v. *Lewis*, 473 A.2d 805, 812 (Del. 1984).
[35] Thomas H. Davenport & Rajeev Ronanki, "Artificial Intelligence for the Real World" 96 *Harvard Business Review* 108 (2018).
[36] Matthew U. Scherer, "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies" 29 *Harvard Journal of Law & Technology* 353 (2016).
[37] *Smith* v. *Van Gorkom*, 488 A.2d 858 (Del. 1985).
[38] Andrew M. Perlman, "The Public's Unmet Need for Legal Services & What Law Schools Can Do About It" 148 *Daedalus* 37 (2019).

to a board that is unable to demonstrate a record of informed inquiry into AI risks, as courts, particularly in Delaware, are increasingly inclined to investigate the deliberative process.[39]

The Obligation of Oversight: From "Caremark" to "Algorithmic Caremark"

Perhaps the most potent legal leverage for AI governance is the obligation to supervise. *In re Caremark International Inc*., Derivative litigation obligation was most effectively articulated.[40] *Caremark* determined that a board of directors must ensure that the company has the appropriate information and reporting systems in place to provide senior management and the board with timely, accurate information. If the board neglects to do so, it may, in rare instances, be held accountable for a "*sustained or systematic failure of the board to exercise oversight*."[41]

The *Caremark* standard, which was further clarified in subsequent cases such as Stone v. Ritter, establishes a high standard for plaintiffs to satisfy. They must demonstrate that the defendant acted in bad faith.[42] Nevertheless, the rationale behind *Caremark* is directly applicable to the dangers of AI. The type of "*mission-critical*" operational risk that *Caremark* was intended to mitigate is an AI system that operates without adequate monitoring, auditing, and reporting mechanisms.[43] One could argue that a board that permits the use of a high-stakes AI system (such as one for medical diagnosis or autonomous navigation) without any means of verifying its safety, bias, or security flaws is not fulfilling its *Caremark* responsibilities.[44]

This implies that a "*Algorithmic Caremark*" standard has been established. This would imply that directors are obligated to implement the following actions for AI systems that are essential to the mission:

1. Ensure that a reasonable system is in place to collect and report information that can monitor the AI for potential risks to safety, transparency, and fairness.

[39] *Brehm* v. *Eisner*, 746 A.2d 244 (Del. 2000).
[40] *In re* Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996).
[41] *Ibid*. at 971.
[42] Stone v. Ritter, 911 A.2d 362 (Del. 2006).
[43] Robert J. Jackson Jr., "Corporate Governance: The Role of the SEC and the Board", speech delivered at the 26th Annual Tulane Corporate Law Institute (March 27, 2014), *available at*: https://www.sec.gov/news/speech/2014-spch032714rjj(last visited on: 27.06.2025).
[44] Elizabeth Pollman, "Corporate Oversight and Disobedience" 72 *Vanderbilt Law Review* 2013 (2019).

2. Address any "*red flags*" that this system raises, such as evidence of major system failures or unfair outcomes.

A high-risk AI application that lacks an oversight system may be considered an example of a bad faith failure to fulfil one's obligation that satisfies the rigorous *Caremark* test for liability.[45]

AN EXAMINATION OF THE FUTURE OF REGULATION IN THE UNITED STATES, THE EUROPEAN UNION, AND INDIA

The legal risks associated with AI are not isolated incidents. Companies are required to adhere to new and frequently conflicting regulations that govern AI, as they are evolving rapidly worldwide. These critical international strategies are essential for any multinational organisation.

The Risk-Based Approach of the AI Act in the European Union

The European Union has adopted the most comprehensive and aggressive approach with its proposed Artificial Intelligence Act (AI Act).[46] The Act establishes a risk-based framework that categorises AI systems into four categories: unacceptable risk (which are prohibited), high-risk, limited-risk, and minimal-risk.[47]

The primary objective of the Act is to regulate high-risk AI systems, which are employed in critical infrastructure, law enforcement, and employment. A number of stringent requirements must be satisfied by the providers of these systems before they can be sold, including:

- Implementing a risk management system.[48]
- Employing high-quality training data to mitigate bias.[49]
- Maintaining an abundance of technical documentation and logging capabilities.[50]

[45] *Marchand* v. *Barnhill*, 212 A.3d 805 (Del. 2019).
[46] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM (2021) 206 final (Apr. 21, 2021).
[47] Paul Nemitz, "Constitutional Democracy and Technology in the Age of Artificial Intelligence" 379 *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* (2018).
[48] *Supra* note 46, art. 9.
[49] *Supra* note 46, art. 10.

- Ensuring that the appropriate individuals are in charge.[51]

The AI Act is a significant stride towards the establishment of a horizontal regulatory framework for AI. It transforms numerous Responsible AI principles from voluntary best practices to mandatory legal obligations for companies that conduct business in the EU, with substantial penalties for noncompliance.[52] It will have an impact on companies worldwide that sell AI systems to the EU market due to its extraterritorial scope.

The United States: A Sector-Specific, Pro-Innovation Position

The European Union has implemented a comprehensive regulatory framework, whereas the United States has implemented a more fragmented, sector-specific approach. The current policy, as outlined in a variety of executive orders and agency guidance, is to promote innovation while minimising risks within the confines of existing legal frameworks.[53] A critical AI Risk Management Framework (RMF) has been developed by the National Institute of Standards and Technology (NIST).[54] In contrast to the EU AI Act, the NIST RMF is optional, providing organisations with a structured and adaptable approach to "*map, measure, and manage*" AI risks.

Although there is no single "*AI Act*" in the United States, there are regulations that are applicable to specific sectors. For instance, the Equal Employment Opportunity Commission (EEOC) has cautioned that the implementation of artificial intelligence (AI) in the hiring process may violate existing anti-discrimination laws.[55] Financial regulators are also conducting a thorough examination of AI-based credit models to ensure that they adhere to fair lending laws.[56] This presents a significant challenge for businesses in terms of

[50] *Supra* note 46, arts. 11, 12.
[51] *Supra* note 46, art. 14.
[52] *Supra* note 46, art. 71.
[53] Exec. Order No. 13859, 84 *Federal Register* 3967 (Feb. 14, 2019), "Maintaining American Leadership in Artificial Intelligence".
[54] National Institute of Standards and Technology, *AI Risk Management Framework (AI RMF 1.0)* (January 2023), *available at*: https://www.nist.gov/itl/ai-risk-management-framework (last visited on: 27.06.2025).
[55] U.S. Equal Employment Opportunity Commission, *The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees* (May 12, 2022), *available at*: https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence(last visited on: 27.06.2025).
[56] Consumer Financial Protection Bureau, "CFPB Circular 2022-03: Adverse action notification requirements in connection with credit decisions based on complex algorithms" (May 26, 2022), *available*

maintaining an accurate record of the various federal and state laws and agency-specific guidance.

India: Formulating a Master Plan for "Responsible AI for All"

India's approach is still in the works, but it has two main goals: using AI to help the economy grow and dealing with social issues. The government's main policy think tank, NITI Aayog, has put out a number of discussion papers, one of which is the National Strategy for Artificial Intelligence.[57] These papers support the idea of "*AI for All*," which stresses the importance of including everyone and using AI to solve big problems in areas like healthcare, agriculture, and education.

The NITI Aayog papers on governance have suggested principles for Responsible AI that are in line with what most people around the world agree on, which are fairness, openness, and responsibility.[58] India's new data protection law, the Digital Personal Data Protection Act, 2023, has rules that will affect AI, especially when it comes to consent and the right to know about automated decision-making. However, there is still no comprehensive law like the EU's AI Act.[59] India's path suggests a balancing act: it wants to build public trust through responsible governance while also encouraging innovation. This will probably result in a mix of ethical guidelines and rules that apply to specific sectors.

This comparison shows that there is a clear global trend: no matter what kind of regulatory model is used, there is a growing legal expectation that businesses will use AI in a responsible and risk-managed way. This outside pressure strongly supports the internal fiduciary duty to create strong compliance systems.

THE BLUEPRINT: A UNIFORM INTERNAL COMPLIANCE SYSTEM FOR AI

at: https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/ (last visited on: 27.06.2025).

[57] NITI Aayog, *National Strategy for Artificial Intelligence* (June 2018), *available at*: https://www.niti.gov.in/sites/default/files/2019-01/NationalStrategy-for-AI-Discussion-Paper.pdf (last visited on: 27.06.2025).

[58] NITI Aayog, *Responsible AI for All: Adopting the Framework* (Feb. 2021), *available at*: https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf (last visited on: 27.06.2025).

[59] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), sec. 11.

Companies must cease responding to issues and instead establish governance that prevents them from occurring in the first place due to legal constraints imposed by both internal fiduciary obligations and external regulations. Four interconnected pillars should be the foundation of a robust internal compliance framework for AI.

Pillar 1: *A Board of Directors with a Comprehensive Understanding of Technology and Top-Down Governance*

Good governance is the responsibility of the board of directors. AI cannot be entirely the responsibility of IT departments.

- *AI Governance Committee:* A special committee, such as an audit or risk committee, should be established by the board to oversee the company's AI strategy and risk management.[60]
- *Designate a Chief AI Officer or Chief Responsible AI Officer:* This individual should be a senior executive who is responsible for the daily implementation of the AI compliance framework. The AI Governance Committee and the CEO should receive direct reports from them.
- *Board Competence:* The board, either as a whole or within its AI Governance Committee, must possess an adequate level of technical expertise. This does not imply that all directors must possess coding skills; however, they must independently acquire knowledge of AI concepts and risks. It is advisable to have at least one director who is a specialist in technology or data science on the board.

Pillar 2: *AI Impact Assessments (AIIAs) that are conducted in advance*

A comprehensive AI Impact Assessment (AIIA) must be conducted prior to the implementation of any AI system that poses a high risk. This internal due diligence process, which is comparable to an environmental impact assessment, would be necessary prior to the system's implementation.[61]

- *Scope and Purpose:* The AIIA would conduct a systematic assessment of a proposed AI system relative to the FTAS principles. It would document the system's purpose,

[60] Allan C. Thygesen, et.al., "Building the AI-Powered Organization" 97 *Harvard Business Review* 62 (2019).
[61] Animesh Kumar, "The Symbiosis of Artificial Intelligence and Legal Research: An Analysis" 13 (2) *Pragyaan Journal of Law* 12 (2023), *available at*: https://ssrn.com/abstract=5267852 (last visited on: 27.06.2025).

the data sources it employs, the potential biases, the measures taken to make it comprehensible, and the security vulnerabilities it contains.

- *Procedure:* The AIIA should be conducted by a cross-functional team that includes legal, compliance, technical, and business professionals. It is necessary to identify potential risks and implement specific measures to mitigate them prior to the system's implementation. For instance, if an AIIA identifies a high risk of bias in a recruitment tool, it may necessitate additional data balancing, model retraining, or a "human-in-the-loop" review to inform final hiring decisions.
- *Documentation:* The completed AIIA is a critical piece of evidence. It demonstrates to regulators and courts that the board and management took AI risks seriously and managed them in a careful, informed, and proactive manner, which is a strong defence against claims of negligence or lack of oversight.

Pillar 3: *Continuous monitoring and Robust Audit Trails*

The implementation of AI systems does not conclude the governance of AI. The organisation must have the capacity to audit and supervise its AI systems during their operation.

- *Algorithmic Logging:* In accordance with regulations such as the EU AI Act, the organisation is obligated to maintain comprehensive logs for high-risk systems.[62] These logs should encompass critical operational parameters, the data that was employed to make specific decisions, and any significant issues or failures. This results in a "algorithmic audit trail" that is essential for the investigation of incidents following their occurrence and for demonstrating the company's accountability.
- *Performance Monitoring:* It is imperative to establish systems that continuously evaluate the performance of AI in relation to the key risk indicators (KRIs) that have been established. It is imperative that these KRIs encompass assessments of fairness, security, and accuracy. For example, it is crucial to conduct consistent testing of a loan-processing AI to ensure that its approval rates across various demographic groups remain within statistically acceptable bounds. An automatic alert should be issued for review if they exceed these limits.

Pillar 4: *The Comprehensive Corporate AI Policy*

[62] *Supra* note 46, art. 20.

The last pillar is a comprehensive, clear, and company-wide AI Policy that has been officially approved by the board of directors. This document serves as the organization's AI governance constitution.

- *Content:* The policy should explicitly state the company's dedication to Responsible AI and delineate the prerequisites for the other three pillars. It must establish the roles and responsibilities of the AI Governance Committee and Chief AI Officer, establish standards for data handling, model validation, and the procurement of third-party AI systems, and clearly define what constitutes a high-risk AI system. Additionally, the AIIA process must be mandated.[63]
- *Procurement Standards:* The policy must address the substantial risks associated with utilising AI from third-party vendors. It should be stated that any AI system purchased from a vendor must undergo the same rigorous AIIA process as an in-house system, and that contracts with vendors must include robust clauses regarding data rights, transparency, and liability.
- *Training and Culture:* Training programs should be mandatory for all employees who require knowledge of the policy, including developers, business users, and management. The objective should be to establish a corporate culture in which all employees are accountable for the responsible development and utilisation of AI.

This four-pillar framework is a legally sound and comprehensive approach to accomplishing tasks. It transforms abstract concepts into concrete, verifiable actions, establishing a framework that safeguards a business's fiduciary obligations while simultaneously enabling it to innovate with AI in a responsible manner.

SUGGESTIONS AND RECOMMENDATIONS

The analysis urges both legal standard-setters and companies to take action. The subsequent recommendations are intended to be beneficial, supported by empirical evidence, and designed to address the governance deficiencies that were identified.

Management and Boards of Directors

[63] Mark MacCarthy and Kenneth Propp, "A New Model for AI Vendor Accountability" *Brookings Institution*, Nov. 29, 2022, *available at*: https://www.brookings.edu/techstream/a-new-model-for-ai-vendor-accountability/ (last visited on: 27.06.2025).

Immediate Board-Level Education: Similar to financial reporting standards, public company boards should receive formal, consistent training on the risks and governance of AI. This action directly satisfies the duty of care requirement of being informed.

Establish a formal AI governance framework: Companies should not wait for the government to dictate their actions. They should take the lead and establish a framework that is based on the four pillars mentioned above: the establishment of a dedicated governance committee, the requirement of AIIAs for high-risk systems, the implementation of robust monitoring, and the adoption of a formal AI policy. This would demonstrate that they are adhering to the Caremark standard for diligent oversight.

Modify the charters of the Risk and Audit committees: The existing charters of the Risk and Audit committees should be immediately modified to indicate that they are responsible for AI-related risks until a distinct AI Governance Committee is established.

For Legislators and Regulators

Clarify the Director's Responsibility for Technological Oversight: In order to clarify the director's responsibility for technological oversight, corporate law statutes, such as the Indian Companies Act, 2013[64], should be amended. A legislative nudge could expedite the adoption of best practices, but a principles-based approach is preferable to an excessive number of regulations. For instance, commentary could emphasise that the duty of care outlined in section 166(3) encompasses the necessity of exercising caution when implementing large-scale technology.

Provide a "Safe Harbour" for Good-Faith Compliance: In an effort to incentivise the proactive implementation of robust governance, regulators may wish to consider the inclusion of a "safe harbour" provision. This would establish a rebuttable presumption that a company has fulfilled its duty of care if it can demonstrate that it adhered to a recognised and rigorous governance framework (such as the NIST RMF or the four-pillared model outlined in this article) and documented its diligence through a formal AIIA process.[65] This would promote meaningful compliance rather than merely checking boxes.

[64] The Companies Act, 2013 (Act 18 of 2013), sec. 166(3).
[65] Deven R. Desai and Joshua A. Kroll, "Trust but Verify: A Guide to Auditing Automated Decision-Making" 31 *Harvard Journal of Law & Technology* 1 (2017).

Enhance the consistency of international standards: Given that AI is being developed and utilised globally, it is imperative that international organisations and national regulators collaborate to ensure that critical governance concepts are more uniform. For instance, they should establish a consensus regarding the definition of "high-risk AI" and the methodology for conducting impact assessments. This would facilitate multinational corporations' compliance with regulations and enhance the predictability of the legal environment.[66]

CONCLUSION

The integration of AI into business operations is a significant transformation, comparable to the industrial revolution or the onset of the internet age. It presents significant opportunities for efficiency and innovation, but it also introduces significant risks and governance issues that exceed the capabilities of conventional legal frameworks. This article has contended that the fundamental principles of corporate law, particularly the fiduciary responsibilities of directors, are not outdated; rather, they require a fresh perspective and a technologically savvy approach.

The passive, reactive approach to AI governance is no longer viable. The powerful imperative for proactive change is created by the spectre of "*Algorithmic Caremark*" liability and the increasing tide of global regulation. The decision for corporate leaders is not whether or not to regulate AI, but rather how. A patchwork of ethical statements and disjointed policies will prove insufficient. An internal compliance architecture that is legally-grounded, integrated, and holistic is necessary to address the challenges of the algorithmic era.

The proposal for a four-pillared framework, which is centred on a comprehensive policy, continuous auditing, proactive impact assessments, and top-down governance, serves as a blueprint for such an architecture. It is a model that is intended to cultivate public trust, ensure accountability, and build resilience. Corporations can exploit the transformative potential of AI in a manner that is not only profitable but also fair, transparent, and accountable to the societies they serve by incorporating responsibility into their internal governance structures, rather than merely mitigating legal risk. The construction of this new governance is one of the most critical tasks that the contemporary corporation must

[66] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* 198 (Oxford University Press, 2020).

undertake, and its successful completion will determine the future of corporate responsibility in the twenty-first century.