

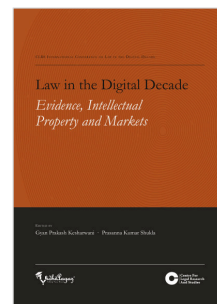
CHAPTER 16

From Corporate Control to Algorithmic Control: Rethinking Directors' Duties and Liability in AI-Driven Corporations

K G Sai Samyukhtha

in *Law in the Digital Decade: Evidence, Intellectual Property and Markets*, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla (VidhiAagaz 2026), pp. 165–176

DOI <https://doi.org/10.63108/VAB.LDD.2.16>



CITATIONS

BLUEBOOK (21ST ED.)

K G Sai Samyukhtha, *From Corporate Control to Algorithmic Control: Rethinking Directors' Duties and Liability in AI-Driven Corporations*, in *LAW IN THE DIGITAL DECADE: EVIDENCE, INTELLECTUAL PROPERTY AND MARKETS* 165 (Gyan Prakash Kesharwani & Prasanna Kumar Shukla eds., VidhiAagaz 2026).

OSCOLA (4TH ED.)

K G Sai Samyukhtha, 'From Corporate Control to Algorithmic Control: Rethinking Directors' Duties and Liability in AI-Driven Corporations' in Gyan Prakash Kesharwani and Prasanna Kumar Shukla (eds), *Law in the Digital Decade: Evidence, Intellectual Property and Markets* (VidhiAagaz 2026) 165.

CHICAGO (17TH ED.)

Samyukhtha, K G Sai. "From Corporate Control to Algorithmic Control: Rethinking Directors' Duties and Liability in AI-Driven Corporations." In *Law in the Digital Decade: Evidence, Intellectual Property and Markets*, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla, 165–176. Maihar: VidhiAagaz, 2026. <https://doi.org/10.63108/VAB.LDD.2.16>.

APA (7TH ED.)

Samyukhtha, K. G. S. (2026). From corporate control to algorithmic control: Rethinking directors' duties and liability in AI-driven corporations. In G. P. Kesharwani & P. K. Shukla (Eds.), *Law in the digital decade: Evidence, intellectual property and markets* (pp. 165–176). VidhiAagaz. <https://doi.org/10.63108/VAB.LDD.2.16>

SOURCE

<https://doi.org/10.63108/VAB.LDD.2.16>

LICENCE

Open access under the Creative Commons Attribution-NonCommercial 4.0 International Licence (CC BY-NC 4.0): it may be copied, shared and adapted for non-commercial purposes, with credit to the authors and the source.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

CHAPTER 16

From Corporate Control to Algorithmic Control: Rethinking Directors' Duties and Liability in AI-Driven Corporations

K G SAI SAMYUKHTHA*

Corporate governance has traditionally assumed that important company decisions are made by human directors, managers, and officers who can be questioned about the reasons for their choices. Artificial intelligence is changing that assumption. AI systems are now used to analyse markets, assess risk, screen employees, detect fraud, forecast demand, recommend investments, and in some settings take actions with little or no human intervention. The legal problem is not simply whether a company may use AI. It is whether existing rules on directors' duties can still allocate responsibility when an important corporate decision is partly or largely produced by an algorithm.

This paper examines that problem mainly through Indian company law, with comparative reference to Delaware, the United Kingdom, the European Union, the OECD and the United States National Institute of Standards and Technology (NIST). Section 166 of the Companies Act, 2013 requires directors to act in good faith, exercise due and reasonable care, skill and diligence, and use independent judgment. These duties remain relevant when AI is used. The difficulty is that the traditional idea of a director as the person who gathers information and then exercises judgment does not fit neatly where an AI system filters information, recommends an outcome, or executes the decision itself.

The paper argues that AI should not become a legal excuse for directors, but directors should also not become automatic guarantors of every error made by a system they did not design or operate. Liability should instead be linked to the degree of AI autonomy, the importance of the decision, the quality of human oversight, the foreseeability of the risk, and the ability of the company and its directors to intervene. The paper proposes an AI Corporate Responsibility Framework with four levels of AI use: assistive, delegated, supervised autonomous, and high-autonomy decision systems. For each level, it proposes a different combination of board oversight, documentation, testing, human review, vendor responsibility, and director liability.

The central conclusion is that the duty of directors should evolve into a clear duty of AI oversight. This duty would require directors to understand the material AI systems used by the company, identify significant risks, establish suitable controls, monitor performance, keep records of important AI-supported decisions, and intervene when a system presents a serious or foreseeable risk. Such a framework protects the basic principle of director accountability while recognising that modern corporate decisions may be produced through a network of directors, employees, software providers, data sources, and autonomous systems.

Keywords: Artificial Intelligence; Algorithmic Decision-Making; Corporate Governance; Directors' Duties; Director Liability; AI Oversight; Corporate Responsibility

1 RESEARCH PROBLEM

The research problem is the mismatch between a legal system built around human corporate judgment and corporate systems that increasingly rely on algorithmic recommendations and autonomous action.

* VIT School of Law, Vellore Institute of Technology, Chennai, Tamil Nadu, India.

Existing company law can usually identify the company, its directors, officers, employees, and service providers. It is less clear how responsibility should be divided when an AI system materially changes the information available to a board or acts without a director making the immediate decision. The problem becomes sharper when an AI system makes a decision that is commercially reasonable in ordinary circumstances but harmful in a particular case, or when the board knew that the system was unreliable but continued to use it.

1.1 Problem Statement

The present legal framework does not clearly state how director duties should operate across different degrees of AI autonomy. If directors are held responsible for every AI error, the law may discourage useful technology and impose an unreasonable burden on individuals. If directors can avoid liability by saying that an algorithm made the decision, the basic purpose of corporate oversight is weakened. The legal gap is therefore not a simple absence of AI legislation. It is an allocation problem: which actor should bear responsibility for a harmful AI-supported corporate decision, and what level of oversight should the law reasonably expect from directors?

1.2 Research Objectives

- To examine how directors' duties under Indian company law apply when AI systems are used in corporate decision-making.
- To identify the circumstances in which directors may be liable for AI-related corporate harm and the circumstances in which liability should fall primarily on other actors.
- To compare the Indian position with selected approaches in Delaware, the United Kingdom, the European Union, and international AI governance frameworks.
- To assess whether existing duties of care, good faith, independent judgment, and oversight are sufficient for AI-driven corporate governance.
- To propose a practical AI Corporate Responsibility Framework that connects the level of AI autonomy with the level of human oversight and legal responsibility.

1.3 Research Questions

- How do existing directors' duties apply when an AI system materially influences or makes a corporate decision?
- When should a director be held liable for harm caused by an AI system used by the company?
- Can a director rely on an AI system in the same way that a director may rely on human officers, experts, or professional advisers?
- What can Indian corporate law learn from Delaware oversight doctrine, UK corporate governance, the EU AI Act, and international AI risk frameworks?
- What legal and governance structure can distribute responsibility between directors, companies, employees, and AI providers without weakening director accountability?

1.4 Methodology

This paper uses doctrinal and comparative legal research. The doctrinal part examines statutory provisions, judicial decisions, and established principles concerning directors' duties, oversight, delegation, and corporate responsibility. The principal Indian source is the Companies Act, 2013, especially section 166. The comparative analysis considers Delaware fiduciary and oversight law, the UK Corporate Governance Code, the EU Artificial Intelligence Act, the OECD AI Principles, and the NIST AI Risk Management Framework. Recent academic writing on AI and corporate governance is used to identify emerging arguments and areas of disagreement. The paper does not claim that any of these frameworks creates a complete legal answer to AI-driven corporate liability. Instead, it uses them to build a workable model for Indian corporate governance.

The method is also normative. After identifying what existing law can already do, the paper asks what additional governance requirements would make the allocation of responsibility fair and workable. The proposed framework is therefore not presented as current Indian law. It is a reform proposal designed to fit within the existing logic of directors' duties.

2 THE BOARDROOM MEETS THE ALGORITHM: INTRODUCTION

Company law has always depended on a practical fiction: a company is a separate legal person, but people must act for it. The board of directors is one of the main human institutions through which that legal person makes choices. Directors decide strategy, approve major transactions, supervise management, monitor risk, and protect the company's interests. Indian company law reflects this model by imposing duties on directors as individuals. Section 166 of the Companies Act, 2013 requires a director to act in good faith, exercise due and reasonable care, skill and diligence, and exercise independent judgment.¹ The assumptions behind these duties are now under pressure. A company may use AI to decide which customers receive credit, which transactions should be blocked, how much inventory should be purchased, which employees should be shortlisted, or which risks deserve management attention. In more advanced systems, software may not merely recommend an outcome. It may take an action automatically after receiving data from other systems. The human director may therefore supervise a process rather than make each decision directly.²

The change is important because corporate law generally allocates responsibility through human roles. A director can be asked what information was considered, why a particular course was chosen, whether alternatives were examined, and whether reasonable precautions were taken. An AI system does not fit comfortably into that model. It has no legal personality as a director, no fiduciary duty to the company, and no independent legal judgment in the corporate-law sense. It is a tool or system deployed by human and corporate actors. That does not mean the tool is legally irrelevant. Its design, data, level of autonomy, contractual terms, monitoring arrangements, and known limitations may all affect whether the human actors acted reasonably.

This is why the question should not be framed simply as "Who is liable when AI makes a mistake?" The better question is "Who made the conditions under which the AI was allowed to act, and what

¹ Companies Act, 2013, No. 18 of 2013, § 166(2)–(3) (India).

² See Deirdre Ahern, *Directors' Duties in the Age of Agentic Artificial Intelligence*, Cambridge Forum on AI: Law and Governance (2026).

safeguards were reasonably required?” This moves the analysis from the final algorithmic output to the governance process that produced it. Recent scholarship increasingly takes this approach, treating AI oversight as an extension of existing fiduciary and care duties rather than as a wholly new area of law.³ The Indian position is especially interesting because section 166 already contains language that can accommodate technological change. The requirements of care, skill, diligence, and independent judgment are open-textured. They can respond to new business practices without requiring a separate statutory duty for every technology. The harder question is how far those words should extend when a director reasonably relies on a complex system whose internal operation the director cannot fully understand.⁴

This paper therefore starts from a modest proposition: AI does not remove the director from the legal picture. Instead, it changes the director’s task. A director who once had to review information personally may now have to govern the information system that produces it. A director who once approved a decision may now have to approve the conditions under which an automated system is permitted to make decisions. In that sense, the central shift is from direct control to supervised control.

3 FROM HUMAN JUDGMENT TO ALGORITHMIC DECISION-MAKING

3.1 The Changing Corporate Decision Process

AI in a corporation exists on a spectrum. At one end, a system may simply organise information or produce a report. The director remains the clear decision-maker. At the other end, an AI agent may receive a goal, gather information, select between options, communicate with other systems, and execute actions. Between these points are systems that recommend decisions, systems that make routine decisions subject to human review, and systems that can act unless a human intervenes.

This spectrum matters legally. The more autonomous the system, the weaker the argument that the director personally made the immediate decision. At the same time, greater autonomy creates a stronger need for governance before the system is deployed. A board that deliberately gives an AI system authority to make high-impact decisions cannot reasonably treat the system as an ordinary piece of office software.

Corporate governance literature already treats boards as bodies responsible for strategy, risk, compliance, and oversight. The same reasoning applies when AI becomes part of those functions. The UK Corporate Governance Code 2024, for example, places strong emphasis on board leadership, division of responsibilities, audit, risk, and internal control. It does not create a special “AI director” role, but its structure is capable of covering AI risk as part of corporate risk and control.⁵ The NIST AI Risk Management Framework similarly treats AI risk management as a continuous process organised around the functions of govern, map, measure, and manage. Although NIST is not a corporate law statute, its structure is useful because it shows how a company can convert general responsibility into repeatable governance practices.⁶

³ See Martin Petrin, *AI Accountability from the Outside In: Corporate Liability, AI Governance, and Managerial Duties*, ECGI Working Paper No. 935 (2026).

⁴ Companies Act, 2013, No. 18 of 2013, § 166(3) (India).

⁵ Financial Reporting Council, *UK Corporate Governance Code 2024* (Jan. 22, 2024).

⁶ Elham Tabassi, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1 (2023).

3.2 Why Algorithmic Error Is Different

An ordinary human error and an algorithmic error can look similar at the end of the process, but their causes may be very different. A human manager may misunderstand a document. An AI system may produce an inaccurate result because its training data was incomplete, because a model changed after deployment, because a data pipeline was corrupted, because a proxy variable created discriminatory outcomes, or because the system was used outside the setting for which it was tested. A director may not have caused the technical failure, but the director may still have been responsible for choosing the system, approving its use, setting its limits, or failing to investigate warning signs.

That distinction suggests a process-based approach to liability. The court should ask what the board knew, what the board could reasonably have known, what the company was using the system for, what controls existed, whether the system had been tested, whether there was a meaningful human override, and whether the risk was material to the company's business. This approach is closer to the traditional duty of care than a rule that simply attaches liability to the person whose name appears on the board.

4 WHAT EXISTING LAW ALREADY SAYS ABOUT DIRECTORS' DUTIES

4.1 India: Section 166 and the Human Director

Section 166 is the starting point for an Indian analysis. A director must act in good faith to promote the objects of the company and in the best interests of the company, its members, employees, shareholders, the community, and the protection of the environment. The director must also exercise due and reasonable care, skill and diligence and independent judgment.⁷ The language is broad enough to cover AI-related conduct without treating AI as a legal person. If a board approves an AI system for a material function, the directors can be expected to consider whether the system is suitable for that purpose, whether the company can monitor it, and whether important decisions can be reviewed or reversed.⁸

Independent judgment is particularly important. Reliance on technology does not automatically mean that a director has given up independent judgment. Directors routinely rely on financial statements, lawyers, auditors, engineers, consultants, and management reports. The legal issue is whether the reliance was reasonable. If the director treats an AI output as automatically correct despite obvious limitations, the problem is not the use of AI itself. The problem is the absence of independent judgment.

The same reasoning applies to diligence. Due diligence in an AI-dependent company may include asking what data the system uses, what its known failure modes are, how often it is tested, who can change its parameters, what happens when it produces an abnormal result, and whether the company has retained enough human expertise to challenge it. A director need not become a software engineer. But a director cannot reasonably remain unaware of a technology that performs a material corporate function.

4.2 Delegation and Reliance

Corporate law accepts that directors cannot personally perform every task. They govern through executives, committees, employees, and outside advisers. This creates a useful comparison with AI. If a director may rely on a chief financial officer or an external auditor in appropriate circumstances, it would be

⁷ Companies Act, 2013, No. 18 of 2013, § 166(2)–(3) (India).

⁸ Id. § 166(3).

strange to say that reliance on a technological system is always forbidden. But AI reliance differs in one important respect: the system may not be a legally accountable professional with a duty to the company. A director therefore has to examine the chain behind the output.

A sensible legal rule is that reliance should be stronger where the AI system is narrow, tested, explainable enough for its purpose, and subject to effective human review. Reliance should be weaker where the system is opaque, self-modifying, connected to external systems, capable of taking irreversible action, or used for decisions involving substantial legal, financial, or human consequences.

4.3 The Comparative Lesson from Delaware

Delaware provides a useful comparison because its corporate law places substantial weight on board process and oversight. The Caremark line of cases developed the idea that directors may face liability for a sustained failure to exercise oversight, particularly where they fail to establish or monitor systems designed to bring important risks to the board's attention.⁹ In *Marchand v. Barnhill*, the Delaware Supreme Court stressed that a board-level monitoring system can be especially important when a risk is central to the company's business. The lesson for AI is not that every algorithm requires a Caremark claim. It is that boards cannot treat a central risk as somebody else's problem when they have the power and responsibility to oversee it.¹⁰

The comparison is useful because AI can create both ordinary business risks and compliance risks. A pricing model that loses money may primarily raise a business judgment issue. An automated system that repeatedly violates privacy law, discriminates against protected groups, or creates serious safety risks may instead raise an oversight issue. The legal analysis should therefore distinguish between a bad result and a governance failure.

5 WHO SHOULD PAY WHEN THE ALGORITHM GOES WRONG?

5.1 The False Choice between Director Liability and No Liability

The strongest temptation in AI liability debates is to choose one responsible party. If the algorithm caused the harm, some may say the software developer should be liable. Others may say that the company owns the system and must therefore bear the loss. Still others may argue that the directors approved the system and should be personally liable. Each position is too simple when used alone.

A corporation can be responsible even when no individual director is personally at fault. A vendor can be responsible for defective software or false representations. Employees can be responsible where they knowingly misuse a system. Directors can be responsible where they fail to exercise the care or oversight required by their role. These forms of responsibility can coexist.

5.2 The Allocation Factors

- Control: Who selected the system, set its purpose, and decided how much authority it had?
- Knowledge: What did the relevant actor know about the system's limitations, failures, and risks?
- Foreseeability: Was the harm a reasonably foreseeable consequence of the system's use?

⁹ *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006).

¹⁰ *Marchand v. Barnhill*, 212 A.3d 805, 821 (Del. 2019).

- **Materiality:** Was the AI system involved in a decision that was important to the company, its finances, compliance, or stakeholders?
- **Autonomy:** Did the system merely advise a human, or did it act without meaningful human approval?
- **Intervention:** Could a human reasonably detect, stop, or reverse the system's action?
- **Documentation:** Did the company keep records showing how the system was tested, monitored, and used?
- **Vendor responsibility:** Did the supplier make material representations about the system's accuracy, safety, or compliance, and were those representations reasonable to rely upon?

These factors help separate a director's personal liability from corporate liability. Suppose a board approves a widely used commercial fraud-detection system after obtaining expert assurance, conducting testing, setting conservative thresholds, and requiring human review of high-risk cases. If a rare and unforeseeable model failure later causes loss, personal director liability should be difficult to establish. Now change the facts: the board knows the system has repeatedly generated false results, removes the human review to save costs, and gives the system authority to block customers automatically. A later harm would be much more difficult to defend as a mere technological accident.

5.3 The EU Approach and Its Relevance to Corporate Governance

The European Union's AI Act takes a risk-based approach and places specific obligations on providers and deployers of certain AI systems. The Act does not replace company law or create a general rule that directors are personally liable for AI outcomes. Its importance for corporate governance lies in its emphasis on risk classification, human oversight, technical documentation, monitoring, and accountability.¹¹ The EU approach therefore supports a broader principle: legal responsibility should increase with the risk and autonomy of the system. This is compatible with, rather than contrary to, the Indian duty of care.¹²

6 COMPARATIVE MODELS FOR AI OVERSIGHT

6.1 United Kingdom: Board Responsibility through Risk and Control

The UK Corporate Governance Code 2024 does not create an AI-specific director duty. Its significance is structural. The Code treats board leadership, division of responsibility, audit, risk, internal control, and reporting as core governance areas. From 2026, Provision 29 requires boards within its scope to make a declaration concerning the effectiveness of material internal controls.¹³

For AI-driven corporations, this suggests that AI should be treated as part of the company's internal control environment when it performs a material function. A board should know where important AI systems are used, who owns each system internally, what risks have been identified, and what controls exist. The UK model is valuable because it does not depend on creating a new category of corporate officer for every new technology.

¹¹ Regulation (EU) 2024/1689, 2024 O.J. (L 1689) 1 (Artificial Intelligence Act), arts. 1, 9–15.

¹² *Id.*

¹³ Financial Reporting Council, UK Corporate Governance Code 2024, Provision 29 and related guidance (2024).

6.2 OECD: Accountability and Human Oversight

The OECD AI Principles, updated in 2024, emphasise transparency and explainability, robustness and security, and accountability. They also call for human agency and oversight appropriate to the context and for traceability across the AI system lifecycle.¹⁴

These principles translate well into corporate governance. A director cannot oversee an AI system if the company does not know what data enters it, what model is being used, who can change it, what outputs it produces, and what happens after an output is generated. Traceability is therefore not only a technical concept. It is also evidence for corporate accountability.

6.3 NIST: A Practical Risk Management Model

The NIST AI RMF 1.0 uses four broad functions: Govern, Map, Measure, and Manage. It is voluntary and not a legal standard, but it provides a practical structure for converting broad responsibility into procedures.¹⁵

In a corporate setting, “Govern” can mean assigning board and management responsibility. “Map” can mean identifying AI systems, their uses, affected stakeholders, data sources, and foreseeable risks. “Measure” can include testing accuracy, bias, security, robustness, and performance. “Manage” can include mitigation, human review, incident response, suspension, and retirement. The value of such a model is that it creates a record of what the company actually did.

6.4 The Indian Gap

India has a strong general corporate law framework, but it does not yet have a single corporate-governance statute that sets out a detailed board protocol for AI systems. This does not mean there is no law. Section 166, securities obligations, data protection rules, consumer law, sectoral regulation, contractual law, and general principles of negligence and corporate responsibility can already apply depending on the facts. The gap is more specific: there is no settled method for translating the general duty of care into expectations for AI selection, testing, monitoring, and intervention.

7 A PROPOSED AI CORPORATE RESPONSIBILITY FRAMEWORK

The paper proposes a four-level AI Corporate Responsibility Framework. The framework is not intended to make AI itself a legal person. It is intended to classify the relationship between the company, its directors, and the AI system so that the level of oversight matches the level of risk.

7.1 Level I — Assistive AI: The Director Decides

At Level I, AI provides information, summaries, forecasts, or recommendations, but a human director or officer makes the actual decision. Examples include board briefing tools, financial analysis, market research, and document review. Director responsibility remains close to the ordinary duty of care. The director should assess whether the information is reliable enough for the decision and should not blindly accept an output merely because it is computer-generated.

¹⁴ OECD, OECD AI Principles (updated 2024).

¹⁵ Elham Tabassi, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (2023).

Controls should include basic source checking, disclosure that AI was used where appropriate, and a rule that material decisions cannot be justified solely by saying “the AI recommended it.”

7.2 Level II — Delegated AI: The System Decides Routine Matters

At Level II, AI is authorised to make defined decisions within limits. Examples may include routine fraud flags, inventory reordering, standard customer service actions, or low-value transaction approvals. The board does not make each decision, but it approves the system’s authority.

Here the director’s duty shifts toward system governance. The board should approve the purpose, limits, escalation rules, and monitoring arrangements. The company should maintain logs and periodically test whether the system remains within its approved purpose. If the board knows that the system regularly exceeds its limits and does nothing, director exposure should increase.

7.3 Level III — Supervised Autonomous AI: The System Acts, Humans Monitor

At Level III, an AI system can make material decisions and act without immediate approval, but a human remains responsible for monitoring and intervention. This level is likely to become more important as agentic systems become capable of carrying out multi-step tasks.

At this level, the company should have a named executive owner, board-level reporting for material systems, documented risk assessments, testing before deployment, ongoing monitoring, incident reporting, a meaningful override mechanism, and clear rules for suspension. Directors should receive enough information to understand the system’s role and risk even if they do not understand its source code.

This approach is consistent with the broader direction of modern AI governance, which places weight on human oversight, traceability, risk management, and the ability to intervene when a system behaves in an unsafe or unexpected way.¹⁶

7.4 Level IV — High-Autonomy AI: The System Can Create Material Corporate Consequences

Level IV covers systems that can take significant financial, legal, operational, or stakeholder-facing actions with little human involvement. Examples could include an agent authorised to negotiate and enter contracts, allocate large amounts of capital, change material pricing, or make decisions with serious consequences for employees or customers.

These systems should face the strongest controls. The board should expressly approve their use. The company should conduct periodic independent audits, maintain detailed decision logs, test for failure and misuse, define prohibited actions, and ensure that the system can be stopped. Material changes to the system should trigger a fresh risk assessment rather than being treated as routine software maintenance.

7.5 The Proposed AI Oversight Duty

The four-level model supports a general AI oversight duty within the existing duty of care. The duty would contain five basic elements: identification, assessment, control, monitoring, and intervention.

- Identification — directors should know which AI systems perform material corporate functions.

¹⁶ OECD, OECD AI Principles (updated 2024); Regulation (EU) 2024/1689, arts. 9–15; NIST, AI RMF 1.0.

- **Assessment** — directors should consider the system’s purpose, reliability, data, autonomy, legal risks, and foreseeable harms.
- **Control** — directors should ensure that authority is limited to what the company has approved and that responsibility is assigned.
- **Monitoring** — directors should receive meaningful reports about failures, unusual outputs, incidents, and material changes.
- **Intervention** — directors should ensure that the company can suspend, correct, or replace a system when serious risk appears.

7.6 When Should Directors Be Personally Liable?

Personal liability should not arise simply because an AI system produced a harmful result. The better test is whether the director breached the applicable duty in relation to the company’s use of the system. Liability becomes stronger where the director approved a high-risk system without reasonable inquiry, ignored known failures, failed to establish basic controls, allowed an autonomous system to act beyond its approved purpose, or failed to respond to material warning signs.

Conversely, liability should be weaker where the company used a system for a legitimate purpose, performed reasonable testing, obtained competent advice, maintained suitable controls, monitored the system, and responded appropriately to incidents. Corporate law should leave room for genuine business risk. The purpose of a duty of care is not to make directors insurers against every loss.

7.7 Responsibility of AI Providers and Other Actors

The framework also recognises that directors do not control every part of an AI system. A software provider may control the model architecture; a data supplier may control training or input data; an employee may configure the system; and an outside consultant may make important representations about performance. Contracts should therefore identify responsibility for testing, security, updates, incident reporting, data quality, and material changes.

However, contractual allocation should not be used to erase the board’s governance role. A director cannot avoid an internal corporate duty merely by signing a vendor agreement. The agreement can allocate operational responsibility, but the board still has to decide whether the company should rely on the system.

7.8 Documentation as a Legal Safeguard

Documentation should be treated as part of governance, not as paperwork added after an incident. For material AI systems, the company should retain a short record of the system’s purpose, level of autonomy, risk assessment, testing, responsible persons, human-override arrangements, known limitations, major incidents, and significant changes.

This protects both the company and directors. If the system later causes harm, the record can show whether the board acted reasonably at the time. It also discourages hindsight-based judgments. A good governance record does not guarantee immunity, but it makes the decision-making process visible.

8 CONCLUSION: KEEPING HUMAN ACCOUNTABILITY IN AN AUTOMATED CORPORATION

AI does not make directors' duties obsolete. It changes what responsible directorship looks like. The traditional director was expected to obtain information, assess it, ask questions, make a decision, and supervise implementation. In an AI-driven company, part of that work may be performed by a system. The director's responsibility therefore moves upward: from checking every individual output to governing the system that produces the outputs.

Indian company law already contains much of the legal foundation needed for this change. Section 166 requires good faith, care, skill, diligence, and independent judgment. Those duties are sufficiently flexible to apply to technology that did not exist when the Companies Act was enacted. What is missing is a clearer understanding of how those duties operate when AI is material, autonomous, and capable of producing decisions at scale.

Comparative developments support a process-based answer. Delaware's oversight cases show why boards must pay attention to important risks and maintain appropriate systems of oversight. The UK governance framework places risk and internal control within the board's responsibility. The EU AI Act uses a risk-based structure and requires governance measures for certain AI systems. The OECD Principles stress accountability, transparency, human oversight, robustness, and traceability. NIST offers a practical risk-management structure. None of these frameworks provides a complete Indian solution, but together they show that AI governance is becoming part of ordinary organisational responsibility.¹⁷

The proposed AI Corporate Responsibility Framework therefore rejects two extreme positions. The first is that directors should remain fully liable simply because they are directors. The second is that directors should escape responsibility because "the algorithm decided." Neither approach reflects how modern corporations actually operate. Responsibility should follow control, knowledge, foreseeability, materiality, autonomy, and the quality of oversight.

The framework's four levels—assistive, delegated, supervised autonomous, and high-autonomy—provide a simple way to connect the level of AI freedom with the level of corporate oversight. At low levels, ordinary professional judgment may be enough. As autonomy and risk increase, stronger testing, monitoring, documentation, board involvement, human override, and independent review should be required. The legal consequence is not automatic director liability. Instead, failure to meet the level of oversight reasonably expected for the system should become evidence in assessing whether a director breached the existing duty of care.

This approach also preserves the separate legal personality of the corporation. AI need not be made a director, officer, or legal person merely because it performs a task that once required a human. Making software a legal director would not solve the real problem because the system cannot bear fiduciary duties in the same way as a human office-holder. The more useful response is to keep human and corporate responsibility in place while recognising that decision-making is increasingly distributed across people, software, data, and vendors.

Ultimately, the central principle should be simple: a director should not be punished for using AI responsibly, but a director should not be permitted to use AI as a shield against responsibility. The law should ask whether the director understood the role of the system, assessed its risks, put suitable controls

¹⁷ Stone v. Ritter, 911 A.2d 362, 370 (Del. 2006); Financial Reporting Council, UK Corporate Governance Code 2024; Regulation (EU) 2024/1689; OECD, OECD AI Principles (updated 2024); NIST, AI RMF 1.0.

in place, monitored material performance, and acted when warning signs appeared. If those steps were taken, an unexpected AI failure should not automatically become personal liability. If those steps were ignored, the fact that an algorithm produced the final output should not break the chain of accountability.

The future of corporate governance is therefore unlikely to be a choice between human control and machine control. It is more likely to be a system of human responsibility exercised through increasingly autonomous tools. The law should adapt to that reality without abandoning the reason directors have duties in the first place: someone must remain answerable for how the corporation chooses to act.

* * *