ARTICLE

AI Governance and Algorithmic Accountability: A Framework for Boards, Company Secretaries and Capital Markets

Artificial Intelligence has quietly moved from being a boardroom enabler to being part of the decision itself, and that shift is exactly why algorithmic governance now sits on the agenda of boards and executive committees rather than being left to the IT department. This article looks at what that means in practice: how AI is reshaping Corporate Governance and capital markets, where unchecked adoption creates legal and ethical exposure, and what a workable framework for evaluating and governing AI deployment actually looks like. Drawing on Indian statutes alongside global governance practice, it is written as a working guide for Company Secretaries and corporate leaders who need to keep fiduciary responsibility and transparency intact while their organisations lean more heavily on automated decision-making.

CS Amit Kumar Sharma, FCS
Practising Company Secretary
Ghaziabad, Uttar Pradesh
fcsasharma@gmail.com

INTRODUCTION

A decade ago, Artificial Intelligence in the boardroom typically meant a fraud-detection system running quietly in the back end of a bank's transaction engine useful, but invisible. Today it drafts the board meeting agenda, auto-approves credit limits, and flags a suspicious trade before a human analyst has even opened the terminal. That change in speed and scope is precisely why AI has become central to how modern corporations actually make decisions, rather than a tool that merely supports them.

For Company Secretaries, legal advisors, and board members, the legal and governance questions around AI matter more than most technology topics precisely because it is the Company Secretary who has to satisfy the board that statutory compliance, capital-market disclosures, and obligations to shareholders are all being met. An ill-designed trading model, a credit-scoring algorithm that quietly discriminates, or a generative AI tool that invents a statistic for a board report — each of these can cause real legal and financial harm, and none of them announces itself in advance. Effective AI governance is, therefore, not about restraining technology for its own sake. It is about making sure the technology serves the corporation's needs without quietly working against the people it is meant to serve.

DEFINING AI AND ALGORITHMIC GOVERNANCE

Governing AI well does not require a computer science degree. What it does require is a functional grasp of what these systems actually do, the terms below are the vocabulary most governance professionals will need day to day:

- **Artificial Intelligence (AI):** Systems that perform tasks (classification, prediction, content creation, recommendations, etc.) requiring human cognitive ability through learning from data, as opposed to following explicitly programmed logic
- **Machine Learning (ML):** A set or sequence of algorithms that identify patterns in historical data for the purpose of making predictions or scores
- **Generative AI (Gen AI):** Algorithms able to create texts/images/video in real time, used for contract language generation, board meeting materials, disclosures and other regulated content
- **Predictive Analytics:** Statistical techniques used to make predictions about revenues, litigation outcomes, regulatory interventions and other future events
- **Automated Decision-Making Systems (ADMS):** Systems that make decisions or take action on a regular basis, including automated trading, lending approvals, and regulatory alerts
- **Algorithmic Governance:** Policies, risk controls, reporting lines, and auditing procedures designed to keep AI applications within the confines of legality and regulatory compliance. In effect, algorithmic governance is corporate governance extended to cover the activities and impacts of AI technologies

GOVERNANCE PRINCIPLES AND STRATEGIC BENEFITS

Leave AI ungoverned and the risks of market abuse and regulatory breaches rise with it; put a thoughtful framework around it, and markets tend to become safer

and more transparent instead. The principles below are the ones that recur across almost every credible AI governance framework:

Accountability, Fairness, Transparency, Explainability, Privacy, Security and Reliability. Human Oversight requires explicit assignment of responsibility for model outcomes and decisions mandates periodic testing for discriminatory outcomes and impact on different groups of society requires explainability and audit trails for regulatory and stakeholder disclosure mandates adherence to legal privacy requirements and limitations on processing of sensitive data sets standards for model accuracy, robustness, and stability across market cycles mandates "human in loop" for critical decisions.

STRATEGIC BENEFITS TO BUSINESS AND GOVERNANCE

Grounds for Improved Audit Quality Reduced Corporate Risk Protection of Confidential Information and Assets

Organisations that put these controls in place tend to see: Enhanced market confidence by assuring transparency of disclosures and board decisions reduced exposure to litigation, regulatory intervention and reputational damage improved decision-making through better analytics and more reliable automated operations protection of confidential information and intellectual property from disclosure through automated channels.

Ability to innovate responsibly within the constraints of regulatory compliance and risk appetite.

The 8-Step AI Governance Lifecycle Framework

A useful way to structure this is as an eight-step lifecycle running from the first policy decision through to day-to-day operations:

1. **Policies:** Set the vision and strategy for AI, which includes approved use cases, constraints, and Corporate Governance.
2. **Data Governance:** Ensuring data quality, lineage, and access controls, data privacy laws, and protection of confidential information.
3. **People & Capability:** Assigning responsibilities, building knowledge and capability, and influencing the culture within the organization.
4. **Technology & Architecture:** Choosing the right models, addressing model risks, understanding and controlling supply chain risks, and evaluating third-party tools.
5. **Risk Management:** Identifying risks such as model failure, hallucination, and bias, prioritizing them, and mitigating them.
6. **Independent Audit:** Performing model audits, reviewing training data, system outputs, and ensuring that all decisions are logged and that regulations are followed.
7. **Continuous Monitoring:** Watching the operations, noticing any deviations, logging any user overrides, and raising alerts when something goes wrong.
8. **Statutory Compliance:** Ensuring that operations are compliant with regulations, laws, and standards both locally and internationally and that records are available for audits.

Practical Implementation Enablers

- **Board and Executive Leadership** – Strong presence of governance at the top level provides the needed support for implementing the system within the organization's processes.
- **Cross-Functional Oversight** – Collaborative effort of the legal, secretarial, compliance, IT, risk management and business units.
- **Comprehensive Documentation** – Detailed description of parameters, training data, design assumptions and changes.
- **Iterative Process** – Constant validation and improvement of models in production based on actual market outcomes.

AI IN CORPORATE GOVERNANCE AND STATUTORY OVERSIGHT

No board has the hours to master the technical intricacies of every automated system running underneath it, and that is fine, statutory oversight was never meant to depend on that. What actually makes board governance of AI work is not data-science fluency around the table; it is insisting on standardised operating limits and periodic model audits, and refusing to sign off until those exist.

Compliance functions sit on both sides of this equation, the biggest beneficiaries of AI and at the same time, the ones left holding the risk. RegTech now lets KYC checks, anti-money-laundering screening, contract review, and transaction monitoring run in a fraction of the time manual review used to take. But speed cuts both ways: every automated compliance decision still amounts to a judgment call, and that judgment was made by a system that cannot itself be held accountable in the way a compliance officer can.

For Company Secretaries specifically, the statutory role is shifting shape: less administrative support, more of an assurance function, checking that AI-generated content is accurate before it ever reaches a statutory register or a formal record.

AI IN CAPITAL MARKETS

Of all the areas where AI touches finance, capital markets are where algorithmic oversight is furthest along. Exchange-level surveillance systems already run

pattern-recognition models around the clock, watching for layering, spoofing, wash trading, and the other tell-tale shapes of manipulative order flow and catching them in real time rather than after the fact.

SEBI ALGORITHMIC TRADING SAFEGUARDS (INDIA)

India's securities regulator, SEBI, has built out a framework specifically for retail participation in algorithmic trading. Under it:

- Stockbrokers are principals for algorithmic orders routed through their API, and algorithmic trading firms are their agents.
- All retail algorithmic orders must be assigned a unique exchange-assigned tag for audit control.
- API-based automated trading requires registered infrastructure, including whitelisting of the Ips.

SEBI has not asked brokers to flip a switch overnight. Following its initial consultation, the regulator set April 01, 2026 as the deadline for brokers to complete registration, with mock trading runs and client-onboarding checks built into the transition period along the way. Separately, regulators and institutional analysts are increasingly turning to natural-language-processing tools to catch discrepancies in filings, earnings call transcripts, and disclosures — a layer of scrutiny that simply was not feasible at this scale a few years ago.

> Surveillance is where AI helps the most and draws the least argument, since no human team could scan millions of daily trades for a pattern a well-trained model spots with ease, provided the model itself stays open to inspection.

Trading algorithms are only part of the picture, though, and SEBI's own thinking has moved well beyond them. In June 2025, the regulator put out a consultation paper proposing guidelines for AI and machine learning use across securities markets generally not just algo trading, but the chatbots brokers use for client support, the surveillance tools exchanges run, and the AI/ML models mutual funds increasingly rely on for customer segmentation and risk profiling. What stands out about the paper is how unglamorous its core asks are: a named senior manager accountable for each model, documented testing before deployment and continuous monitoring afterward, disclosure to clients when an AI system materially affects them, and a five-year retention period for model inputs and outputs so that decisions can be reconstructed later if something goes wrong. It also proposes a lighter compliance tier for AI used purely for internal purposes, compliance monitoring, cybersecurity as opposed to AI that touches a client's money or advice directly, which is a sensible bit of proportionality that avoids treating a chatbot the same as a trading algorithm. As a consultation paper rather than a notified regulation, none of this is binding yet, but it is a reasonably clear signal of where SEBI intends to land, and governance teams at brokers, exchanges, and asset managers would do well to start building toward it now rather than waiting for the final circular.[1A]

LEGAL EXPOSURE, STATUTORY RISKS AND NON-DELEGABLE FIDUCIARY DUTY

AI tools assist a decision; they do not make it in any legal sense. No individual or entity can hand its statutory responsibilities off to an algorithm, and no one escapes liability for an act or omission simply because a model was involved somewhere upstream. Used carelessly, these tools can expose an organisation and the individuals signing off on its behalf to serious statutory and regulatory consequences.

LIST OF STATUTES, RULES AND RISK EXPOSURE

1. **SEBI (Prohibition of Insider Trading) Regulations, 2015:**

   Statutory Provisions: Regulation 2(1)(n) (definition of unpublished price sensitive information), Regulation 3 (prohibition of communication of UPSI), and Regulation 3(5) (maintenance of structured digital database).

   Legal Exposure: Communication of Unpublished Price Sensitive Information (UPSI) to any AI platform, including its storage or processing, will be a violation of the aforesaid regulations. Examples of UPSI include, *inter alia*, draft financial statements, board papers, and proposals concerning merger, acquisition, or other business combinations.

2. **SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015:**

   Statutory Provisions: Regulation 4 (Principles governing disclosures and obligations), and Regulation 30 (disclosure of material events).

   Legal Exposure: Unauthorized disclosure or communication of material non-public information on any unauthorized platform.

3. **Companies Act, 2013:**

   Statutory Provisions: *Sections 118* (integrity and proper maintenance of Board Minutes, read with Secretarial Standard-1 on restricted access), 134 (Financial statement, Board's report, etc), 166 (duties of directors to exercise independent judgment and due diligence), and 447 (fraud).

   Legal Exposure: Breach of confidentiality of board meetings, minutes, or other board papers, failure to exercise independent judgment or due diligence by directors, or misstatement in the financial books or statutory records.

4. **Secretarial Standards:**

   Statutory Provisions: SS-1 and SS-2 deal with the confidentiality of board meetings, background papers, resolutions, and general meeting proceedings.

   Legal Exposure: Unauthorized disclosure or processing of secretarial records or papers.

5. **Digital Personal Data Protection Act, 2023 (DPDP Act):**

   Statutory Provisions: The DPDP Act provides for lawful processing of personal data and restricts processing except for specified limited purposes.

   Legal Exposure: Processing of personal data (such as, personal identifiers, employee data, and salary details) on any third-party platform without the consent of the data principal and in violation of the DPDP Act.

6. **Information Technology Act, 2000:**

   Statutory Provisions: Section 43A (compensation for failure to prevent disclosure of information), and Section 72A (criminal liability for disclosure of information in violation of lawful contract).

   Legal Exposure: Failure to protect sensitive personal data or commercial information from unauthorized use or disclosure, or unauthorized commercial use or disclosure of such information, may result in penalties or criminal liabilities.

7. **Indian Contract Act, 1872:**

   Statutory Provisions: Express terms of Non-Disclosure Agreements (NDAs) or other commercial contracts.

   Legal Exposure: Violation of any express term of a contract, such as NDAs, by disclosing any information on any third-party platform/AI tools.

8. **Copyright Act, 1957:**

   Statutory Provisions: Sections 14 (ownership of copyright), and 51 (infringement).

   Legal Exposure: Unauthorized use or reproduction of any copyrighted work, or use of any third-party platform to generate infringing content.

9. **Statutory and Regulatory Professional Conduct Rules:**

   Statutory Provisions: Statutory professional conduct rules for Company Secretaries (ICSI), Chartered Accountants (ICAI), Cost Accountants (ICMAI), and Advocates (Bar Council of India).

   Legal Exposure: Penalty, suspension, or other disciplinary action for violation of professional conduct rules by Company Secretaries, Chartered Accountants, Cost Accountants, or Advocates for disclosure of any information or negligence in their duties.

Safe AI Usage Checklist and Best Practices:

Before uploading anything to an AI tool for advice or analysis, governance professionals should run through this checklist first, not after:

Pre-Upload Safe AI Checklist

[ ] Does the material contain Unpublished Price Sensitive Information (UPSI)?

[ ] Does the document contain undisclosed material corporate events?

[ ] Does the content include identifiable personal data?

[ ] Does the text include confidential board papers or executive agendas?

[ ] Does the file contain proprietary source code or trade secrets?

[ ] Does the proposed usage violate internal enterprise AI policies?

[ ] Can the input data be completely masked, anonymized, or sanitized?

[ ] Will all generated facts, statutory citations, and figures be independently verified?

The Bottom Line: A single "yes" or even "not sure" to any of the above is reason enough to keep that material off a public AI platform.

Operational Red Flags vs. Recommended Practices

High-Risk Actions (Prohibited Practice) DOCX	Recommended Governance Best Practice DOCX
Ingesting real client names or explicit monetary figures into prompts.	Anonymize inputs using generic placeholders (e.g., "Company X").
Uploading trade secrets or unannounced product details.	Completely redact proprietary details before model processing.
Sharing confidential board minutes, notes, or strategy decks.	Maintain sensitive boardroom files strictly within secure internal systems.
Delegating final strategic or legal decisions to automated outputs.	Use AI solely for research assistance while retaining human judgment.
Issuing raw AI-generated text directly to clients, courts, or regulators.	Review, edit, and validate all generated content prior to issuance.
Relying on AI outputs as factually accurate without primary checks.	Verify every claim, figure, and legal citation against primary sources.
Processing personal data using free, open-web AI tools.	Deploy enterprise-grade, secured AI platforms with closed data terms.
Assuming AI systems possess current legal and regulatory knowledge.	Cross-check statutory references against updated legal databases.

Global Comparative Governance Framework

Governance Dimension	Indian Framework	International Standards & Frameworks
Corporate Oversight	Companies Act, 2013; SEBI LODR Regulations, 2015	EU AI Act (Regulation (EU) 2024/1689); OECD AI Principles
Capital Markets	SEBI Algorithmic Trading Directives	EU MiFID II; US SEC Rule 15c3-5 Market Access Rules
Data Protection	Digital Personal Data Protection Act, 2023 & DPDP Rules	EU General Data Protection Regulation (GDPR)
Risk Standards	MCA & RBI Guidance Notes on Technology Risk	NIST AI Risk Management Framework; ISO/IEC 42001:2023
Multilateral Rules	Global Partnership on AI (GPAI); G20 AI Commitments	G7 Hiroshima AI Process; UNESCO Ethics of AI

India: India's stated position, set out in the India AI Governance Guidelines released by MeitY's drafting committee, is that a separate horizontal AI statute is not needed at this stage. The Committee's assessment is that existing law (the IT Act, the Bharatiya Nyaya Sanhita, the DPDP Act, sectoral rules from SEBI, RBI, and others) already reaches most AI-related harms, provided enforcement is timely and consistent. Regulation therefore proceeds sector by sector, through SEBI, RBI, MCA, and MeitY as the nodal ministry, layered on top of horizontal data protection legislation (the DPDP Act, 2023, phasing in through 2025–2027). This is a deliberate choice, not an absence of a framework — it is explicitly closer to the UK's cross-sectoral, principles-based model than to the EU's single binding statute.

European Union: The EU has taken the opposite path a single, horizontal, risk-tiered statute (the EU AI Act) rather than sector-by-sector rules. Ongoing Digital Omnibus reforms have pushed the compliance deadline for standalone high-risk systems under Annex III out to December 2027, though the transparency obligations under Article 50 are already in force and were not part of that deferral.

Five International Frameworks Worth Knowing

The comparative table above names the frameworks; what follows is what each one actually does, and why it belongs on a governance professional's radar even where it carries no direct legal force in India.

EU AI Act (Regulation (EU) 2024/1689) remains the most comprehensive, legally binding regulation of AI to enter into force anywhere. It sorts AI systems into risk tiers unacceptable, high, limited, and minimal and scales obligations accordingly, with the heaviest documentation, testing, and human-oversight requirements falling on high-risk systems such as those used in credit scoring, employment decisions, or critical infrastructure. Its extraterritorial reach means that any Indian company offering an AI-enabled product or service into the EU market, or whose AI system's output is used within the EU, may fall within scope regardless of where the system itself was built.

NIST AI Risk Management Framework (AI RMF 1.0) is voluntary rather than binding, but it has become the de facto reference point for structuring an AI risk programme, including in jurisdictions with no equivalent statute of their own. Its four core functions — Govern, Map, Measure, and Manage give a board a simple vocabulary for asking whether a given AI system is actually under control: who owns it, what could go wrong, how is that measured, and what happens when it does. Indian companies with no obligation to use the AI RMF often adopt it anyway, simply because internal auditors and international clients increasingly expect to see it referenced.

Global Partnership on Artificial Intelligence (GPAI) is not a regulator and issues no binding rules; it is a multistakeholder policy body, formed in 2020 and merged with the OECD in July 2024, that brings together India and roughly forty-five other member countries to develop shared, practical guidance on responsible AI. Its relevance for Indian governance professionals is less about compliance and more about direction of travel — GPAI's working groups on responsible AI and data governance tend to anticipate the themes that later show up in binding regulation elsewhere, India included.

G7 Hiroshima Process on Generative AI grew out of the G7's 2023 Hiroshima Summit and resulted in the Hiroshima Process Comprehensive Policy Framework, agreed in October 2023, which set out International Guiding Principles and a voluntary Code of Conduct specifically for organisations developing advanced, general-purpose, and generative AI systems. It does not bind Indian companies directly, but any organisation relying on frontier foundation models built by G7-based developers is, in practice, relying on systems whose builders have committed to these principles which makes the framework worth understanding even for organisations that only consume AI rather than build it.

ISO/IEC 42001:2023 is the one item on this list that a company can actually get certified against. Published in December 2023, it sets out requirements for an AI management system in much the same structural style as ISO 27001 does for information security — covering policy, risk assessment, resourcing, and continual improvement, auditable by an accredited certification body. For an Indian company that wants to demonstrate credible AI governance to an international counterparty, client, or

regulator without waiting for domestic law to catch up, ISO/IEC 42001 certification is currently the closest thing available to an independently verified stamp of approval.

None of these five frameworks replaces Indian statutory law, and none should be treated as a substitute for legal advice on a specific transaction. What they offer instead is a shared vocabulary and a set of practices that Indian governance professionals can draw on particularly useful in the gap between where domestic AI-specific regulation currently stands and where an organisation's own risk exposure already sits.

INDIA'S OWN FRAMEWORK: THE AI GOVERNANCE GUIDELINES

Beyond the sector-specific statutes discussed above, MeitY's drafting committee released the India AI Governance Guidelines, which set out the government's stated philosophy and proposed institutional architecture for AI oversight. Three parts of it are directly useful for a governance professional.

The seven sutras are seven guiding principles, adapted from the Reserve Bank of India's FREE-AI Committee report (August 2025), that the Guidelines hold out as India's governance philosophy: **Trust is the Foundation, People First, Innovation over Restraint, Fairness & Equity, Accountability, Understandable by Design, and Safety, Resilience & Sustainability**. Read together, they signal a deliberate tilt toward enabling adoption rather than restraining it. The Guidelines state explicitly that, all else equal, responsible innovation should be prioritised over cautionary restraint. That is a real policy choice, not a neutral default, and it is worth knowing when advising a board on how much regulatory headroom India currently affords.

The Guidelines also propose new institutional machinery, though it is not yet operational. An AI Governance Group (AIGG), chaired by the Principal Scientific Adviser, is intended to coordinate policy across ministries and sectoral regulators; a Technology & Policy Expert Committee (TPEC) would brief the AIGG on emerging capabilities and regulatory gaps; and the AI Safety Institute (AISI), which does already exist under the IndiaAI Mission, is positioned as the technical body responsible for testing, standards development, and safety research. Until the AIGG is actually constituted, however, AI governance in India continues to run through existing sectoral regulators — SEBI, RBI and others rather than through a single coordinating body.

On classification and liability, the Guidelines make an admission worth flagging to clients directly: the IT Act's intermediary safe-harbour under Section 79 was built around a model of passive hosting, and the Committee's own assessment is that this immunity likely does not extend to AI systems that generate or modify content. Combined with unresolved questions about how developers, deployers, and users should be classified and how liability should be apportioned between them, this is flagged as requiring legislative amendment not yet enacted, but a live gap rather than a settled question.

DEPA for AI Training is a techno-legal proposal worth knowing about: an extension of India's existing Data Empowerment and Protection Architecture already used for consent-based data sharing in the financial sector into the AI training pipeline, so that personal data used

to train models remains subject to auditable, consent-token-based permissions. The Guidelines are candid that this has real limitations, including a performance cost from privacy-preserving techniques and a limited ability to govern what happens after a model is trained, but it illustrates the kind of compliance-by-design approach India is betting on alongside conventional regulation.

None of this changes the underlying statutory analysis set out earlier in this article. What it does is give governance professionals the vocabulary and institutional map that Indian policy is actually using, useful when a client asks not just "what does the law require today" but "where is Indian AI policy heading, and how quickly."

CONCLUSION

AI adds value to corporate management and capital markets only when real governance controls sit around it, left ungoverned, the same tools that improve decision-making just as easily create new points of failure. Regulators in multiple jurisdictions are converging on similar answers: risk-based model governance, audit trails for algorithm-driven processes, stronger data-privacy protection, and clear accountability when something goes wrong. For boards, legal advisors, and Company Secretaries, the task ahead is not to choose between adopting AI and staying compliant. It is to make sure every algorithm the organisation relies on operates inside the law and to be able to prove it when asked.

REFERENCES:

i. *Codes of professional conduct of the Institute of Company Secretaries of India, the Institute of Chartered Accountants of India, the Institute of Cost Accountants of India, and the Bar Council of India.*

ii. *Companies Act, 2013 (India), Sections 118, 134, 166, and 447.*

iii. *Copyright Act, 1957 (India), Sections 14 and 51.*

iv. *Digital Personal Data Protection Act, 2023 (India); Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India.*

v. *European Commission, proposal for a "Digital Omnibus on AI" amending Regulation (EU) 2024/1689, November 2025; political agreement reached May 2026; formally adopted and signed by the European Parliament and Council, July 8, 2026.*

vi. *G7, Hiroshima Process Comprehensive Policy Framework, including the Hiroshima Process International Guiding Principles and the International Code of Conduct for Organizations Developing Advanced AI Systems, October 30, 2023.*

vii. *Indian Contract Act, 1872.*

viii. *Information Technology Act, 2000 (India), Sections 43A, 72A, and 79.*

ix. *Institute of Company Secretaries of India, Secretarial Standards SS-1 and SS-2.*

x. *ISO/IEC 42001:2023, Information technology — Artificial intelligence — Management system, International Organization for Standardization, December 2023.*

xi. *Ministry of Electronics and Information Technology, Government of India, India AI Governance Guidelines: Enabling Safe and Trusted AI Innovation, drafting committee.*

xii. *National Institute of Standards and Technology (NIST), Artificial Intelligence Risk Management Framework (AI RMF 1.0), U.S. Department of Commerce, January 2023.*

xiii. *OECD, Global Partnership on Artificial Intelligence (GPAI), integrated with the OECD from July 2024; see oecd.ai.*

xiv. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).*

xv. *Reserve Bank of India, Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI Committee Report), August 2025.*

xvi. *SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, Regulations 4 and 30.*

xvii. *SEBI (Prohibition of Insider Trading) Regulations, 2015, Regulations 2(1)(n) and 3.*

xviii. *Securities and Exchange Board of India, Circular on Safer Participation of Retail Investors in Algorithmic Trading (SEBI/HO/ATD/ATD-PoD-2/P/CIR/2025), February 4, 2025, and subsequent circulars extending the implementation timeline to April 1, 2026.*

xix. *Securities and Exchange Board of India, Consultation Paper on Guidelines for Responsible Usage of AI/ML in Indian Securities Markets, issued on June 20, 2025*

This article is for general informational purposes and does not constitute legal advice. Readers should verify current effective dates and provisions directly against SEBI, MeitY, MCA, EU and etc. official sources before relying on this material for compliance decisions.