भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CONSULTATION PAPER ON "GUIDELINES FOR RESPONSIBLE USAGE OF AI/ML IN INDIAN SECURITIES MARKETS"

1. OBJECTIVE

To solicit comments from stakeholders and members of public on the proposed guiding principles for responsible usage of Artificial Intelligence (AI)/ Machine Learning (ML) applications/models in securities markets. These guiding principles are intended to optimise benefits and minimise potential risks associated with integration of AI/ML based applications in securities markets to safeguard investor protection, market integrity, and financial stability. (Definitions of AI and ML are given in Annexure A)

2. BACKGROUND

2.1 SEBI has prescribed reporting requirements for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by Stock Exchanges, Clearing Corporations, Depositories, Intermediaries and Mutual Funds. The intent of the circulars was to create an inventory of the AI / ML landscape in the Indian financial markets to gain an in-depth understanding of the adoption of such technologies in the markets and to ensure preparedness for any AI / ML policies that may arise in the future.

2.2 Further, it has been observed that the usage of AI and ML based applications/models have greatly increased in the financial markets because of better availability of data and computational power, coupled with significant improvements in software and hardware. Further, the field of AI/ML has seen significant advancement due to development of Generative AI (Gen AI) and Large Language Models (LLMs), which has opened up new use cases in financial sector for market participants. AI/ML is being used by market participants mainly for advisory and support services, risk management, client identification and monitoring, surveillance, pattern recognition, internal compliance purpose, cyber security etc. While AI/ML has the potential to improve productivity, efficiency and outcome, it is also important to manage these systems responsibly as their usage also creates or amplifies certain risks which could have an impact on the efficiency

of financial markets and may result in adverse impact to investors. Therefore, SEBI considers it appropriate to devise high-level principles to provide guidance to the market participants for having reasonable procedures and control systems in place for supervision and governance of usage of AI/ML applications/tools. This consultation paper enumerates various emerging risks across several dimensions such as Fairness and Bias, Accountability and Governance, Transparency and Explainability, Monitoring and Operational Resilience, Oversight of third-party vendors, Cyber and Data Security etc. and guiding principles for mitigating those risks.

2.3 In order to study and prepare guidelines for usage of AI/ML applications in the Indian Securities Market, SEBI constituted a working group.

2.4 The terms of reference of the working group was as follows:

a) To study Indian, global best practices.
b) To prepare the guidelines for usage of AI / ML applications.
c) To address the concerns / issues due to use of AI / ML applications.

2.5 The working group studied the existing AI/ML guidelines in India as well as globally. The group also invited various intermediaries such as Stock Exchanges, Brokers and Mutual Funds to explain the use of AI/ML in their organization and respective industries. Subsequently, the working group had multiple rounds of discussions to finalize the guidelines for securities market.

3. STUDY OF INDIAN/GLOBAL BEST PRACTICES

The working group studied the guidelines/principles on use of AI/ML, prescribed / adopted by various domestic and international organizations.

3.1 NITI AAYOG GUIDELINES ON USE OF AI/ML IN INDIA

In India, NITI Aayog released an approach document in February, 2021 – "Principles for Responsible AI" [1]. The paper examines different system

[1] https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf

considerations including privacy and security related risks. On the basis of these system considerations, the paper identifies following broad principles for responsible management of AI:

1. Principle of Safety and Reliability
2. Principle of Equality
3. Principle of Inclusivity and Non-discrimination
4. Principle of Privacy and security
5. Principle of Transparency
6. Principle of Accountability
7. Principle of protection and reinforcement of positive human values

Subsequently, NITI Aayog published a follow up document in August 2021[2], which identifies the various mechanisms needed for operationalizing these seven principles.

3.2 EXISTING IOSCO GUIDELINES ON USE OF AI/ML

Considering the role of AI and ML in financial markets, IOSCO (International Organisation of Securities Commissions) released a consultation paper[3] in June 2020 after conducting surveys and discussions with market intermediaries to identify how AI and ML are being used and the associated risks. Following potential risks and harms were identified which may arise due to use of AI and ML:

- Governance and oversight
- Algorithm development, testing and ongoing monitoring
- Data quality and bias
- Transparency and explainability
- Outsourcing
- Ethical concerns.

[2] https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf
[3] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD658.pdf

Based on the responses received to the Consultation Report, a final report was released in September 2021. This final report provides guidance to assist IOSCO members in supervising market intermediaries and asset managers that utilise AI and ML. Following six measures are proposed in the report –

Measure 1: Regulators should consider requiring firms to have designated senior management responsible for the oversight of the development, testing, deployment, monitoring and controls of AI and ML. This includes a documented internal governance framework, with clear lines of accountability. Senior Management should designate an appropriately senior individual (or groups of individuals), with the relevant skill set and knowledge to sign off on initial deployment and substantial updates of the technology.

Measure 2: Regulators should require firms to adequately test and monitor the algorithms to validate the results of an AI and ML technique on a continuous basis. The testing should be conducted in an environment that is segregated from the live environment prior to deployment to ensure that AI and ML:

i. behave as expected in stressed and unstressed market conditions; and
ii. operate in a way that complies with regulatory obligations.

Measure 3: Regulators should require firms to have the adequate skills, expertise and experience to develop, test, deploy, monitor and oversee the controls over the AI and ML that the firm utilises. Compliance and risk management functions should be able to understand and challenge the algorithms that are produced and conduct due diligence on any third-party provider, including on the level of knowledge, expertise and experience present.

Measure 4: Regulators should require firms to understand their reliance and manage their relationship with third-party providers, including monitoring their performance and conducting oversight. To ensure adequate accountability, firms should have a clear service level agreement and contract in place clarifying the scope of the outsourced functions and the responsibility of the service provider. This agreement should contain clear performance indicators and should also clearly determine rights and remedies for poor performance.

Measure 5: Regulators should consider what level of disclosure of the use of AI and ML is required by firms, including:

i. Regulators should consider requiring firms to disclose meaningful information to customers and clients around their use of AI and ML that impact client outcomes.

ii. Regulators should consider what type of information they may require from firms using AI and ML to ensure they can have appropriate oversight of those firms.

Measure 6: Regulators should consider requiring firms to have appropriate controls in place to ensure that the data that the performance of the AI and ML is dependent on is of sufficient quality to prevent biases and sufficiently broad for a well-founded application of AI and ML.

Further, it was observed by the group that Financial Industry Regulatory Authority of United States (FINRA, USA), Monetary Authority of Singapore (MAS) and Department of Industry Science and Resources of Australia (DISRA) released guidelines to the respective industries which are in line with the aforementioned IOSCO principles.

4. CURRENT USAGE OF AI/ML IN INDIAN SECURITIES MARKETS

4.1 Based on the presentation made by the market participants, the current usage of AI/ML in the Indian Securities Market are as follows:

a) **Exchanges:** AI/ML based technologies are being used by exchanges broadly for Surveillance, advanced cyber security tools, Member Support using Chatbot, automating data input tasks for Member Compliance, ML algorithms to process vast amount of data, social media analytics, pattern recognition etc.

b) **Brokers:** Brokers are leveraging AI/Ml based technologies mainly for KYC/Document processing, Product Recommendation, Chatbot, Digital Account Opening, Surveillance, Anti-money laundering, Order execution and Product Propensity.

c) **Mutual Funds:** Mutual fund are leveraging AI/ML tools mainly for customer support services such as Chatbots, Cyber security, Surveillance tools, Customer Segmentation etc.

5. RECOMMENDATIONS OF THE WORKING GROUP

The working group gave its recommendations to implement appropriate guardrails, continuous monitoring and human-in-the-loop throughout the development and deployment lifecycle for responsible usage of AI/ML in securities markets. The report of Working Group was placed before Committee on Financial and Regulatory Technologies (CFRT) of SEBI.

This consultation paper has been prepared based on the recommendations of the Working Group, suggestions of CFRT, discussions with market participants and internal deliberations. These guidelines are broadly based on following core guiding principles for responsible usage of AI/ML:

5.1 Model Governance
5.2 Investor Protection-Disclosure
5.3 Testing framework
5.4 Fairness and bias
5.5 Data Privacy and Cyber Security measures

5.1 Model Governance

a. Market participants using AI/ML models[4] should have an internal team with adequate skills, expertise and experience to monitor and oversee the performance, controls, testing, efficacy, and security of the algorithms deployed throughout their lifecycle as well as maintain auditability and explain ability/interpretability of AI/ML based models. This shall also include documentation of model development, validation, model versioning and ability to do replay for diagnosis etc.
b. The team should implement appropriate risk controls measures and governance frameworks to oversee and challenge the outcomes derived from the AI/ML models (especially during market stress). The team should

[4] The term model is used interchangeably with application, algorithm, tools and technique in this consultation paper

assess and manage potential risks on a continuous basis to ensure that AI/ML models function in a robust and resilient way. The robustness of AI/ML systems can be reinforced by careful training, and retraining, of ML models with datasets large enough to capture non-linear relationships and tail events in the data.

c. The team should establish procedures for exception and error handling related to AI/ML based systems. The team should also establish back-up/fall back plans in the event an AI based application fails (e.g. due to technical issue or an unexpected disruption) to ensure that the relevant function is carried out through an alternative process.

d. There should be a designated senior management, having appropriate technical knowledge and experience, responsible for the oversight of the model development, validation, ongoing testing, deployment, monitoring and controls of AI/ML based models.

e. Market participants shall understand their reliance on and manage their relationship with third-party service providers/vendors of AI and ML, including monitoring providers' performance and conducting oversight. Market participants should have a clear service level agreement and contract in place with third-party vendors clarifying the scope of the outsourced functions, performance indicators and clearly determining their rights and remedies for poor performance by vendors. However, AI and ML services provided by third-party vendors are deemed to be provided by the market participants, who shall be responsible for ensuring compliance with all applicable laws, rules and regulations.

f. Since AI/ML applications can learn from live data and their model behaviour may hence change after deployment, market participants should conduct periodic reviews and on-going monitoring to ensure that the applications continue to perform as intended. Further, market participants shall share accuracy results of AI/ML models with SEBI on periodic basis.

g. Market participants should clearly define data governance norms which inter-alia shall include data ownership, access controls, encryption

mechanism, rights etc. Any requests for unmasking of data shall be recorded.

h. AI/ML based systems and its use/test cases shall be subjected to independent auditing (team that has no role in development) mechanisms to ensure transparency and fairness. Audit findings shall be communicated to SEBI to enable proactive monitoring and supervisory oversight.

i. While devising AI/ML based applications, market participants should provide for users' autonomy and agency in decision-making processes and develop AI models that are sensitive to diverse cultural backgrounds and values.

j. Market participants should ensure responsible and ethical outcomes in usage of AI/ML against clearly defined rules and practices.

k. Market participants should retain and adequately secure logs for AI/ML systems with full verbosity so that it is possible to chronologically reconstruct the occurrence of events.

l. Market participants should have control to switch to manual feedback or auto feedback from time to time basis.

m. The AI/ML models should operate in a way that complies with existing legal and regulatory obligations.

5.2 Investor Protection-Disclosure

a. Market participants using AI/ML models for business operations that may directly impact their customers/clients should disclose the same to the respective customers/clients to foster trust, transparency and accountability. Following is a non-exhaustive list of such operations:

   i. Selection of trading algorithms/Algorithmic trading (including High frequency trading)
   ii. Asset Management/Portfolio Management
   iii. Advisory and support services

b. Further, non-exhaustive list of disclosure of information to investors for usage of AI and ML applications is given below:

i. Product features, purpose, risks involved, limitations and accuracy results of the model.
ii. Fees/Charges to be levied, if applicable
iii. Information about the quality of data that is used to make AI/ML driven decisions including its accuracy, completeness and relevance.

c. The language used in the disclosures should be comprehensible to customers/clients. This will help facilitate customers/clients to understand the service and products that are being offered/sold and allow them to make informed decisions.
d. Investor grievance mechanism for AI/ML systems shall be in line with existing regulatory framework of SEBI

5.3 **Testing framework**

a. The market participants should adequately test and monitor the AI/ML based models to validate their results on a continuous basis.
b. The testing should be conducted in an environment that is segregated from the live environment prior to deployment to ensure that AI/ML models behave as expected in stressed and unstressed market conditions.
c. In addition to the existing methods of testing, market participants should perform shadow testing with live traffic of AI/ML models to ensure quality and performance before deployment in production environment.
d. Market participants should maintain proper documentation of all the models and store input and output data for at least 5 years. Market participants should also maintain proper documentation explaining the logic of AI/ML models to ensure that the outcomes produced are explainable, traceable and repeatable.
e. The behaviour of AI/ML model may change in an unforeseen manner as more data is processed over time. Market participants should think beyond the existing testing methods that may be used for traditional algorithms and ensure the AI/ML models are monitored continuously as the algorithms adjust and transform. Therefore, it is not enough for the AI/ML models to be tested thoroughly before deployment; they need to be

continuously monitored throughout their deployment to ensure that the model does not behave in inexplicable ways owing to a subtle shift in the operating conditions or due to excessive noise.

5.4 **Fairness and Bias**

a. AI/ML based models should be fair. Specifically, they should not favour or discriminate one group of clients/customers over another.
b. As the performance of AI/ML is essentially dependent on the quality on input data and lack of bias in processing, market participants should ensure an adequate level of data quality and it should be sufficiently broad. This may be done by checking the quality of the sources used, as well as the relevance and completeness of the data about the underlying objectives of the model.
c. Market participants should implement appropriate processes and controls to identify and remove biases from data sets. Further, specific training courses to raise awareness amongst their data scientists (and/ or other relevant staff) of potential data biases may be conducted.

5.5 **Data Privacy and Cyber Security**

a. Since the AI/ML systems are dependent on collection and processing of data, Market participants should have a clear policy for data security, cyber security and data privacy for the usage of AI/ML based models.
b. Collection, usage, processing of investors' personal data, security measures etc. should be in compliance with applicable laws.
c. Information about technical glitches, data breaches shall be communicated to SEBI and other relevant authorities, as applicable in line with existing regulatory and legal framework.

Market participants may refer the possible control measures as mentioned in **Annexure B** to manage the risks arising from usage of AI/ML models.

6. TIERED APPROACH

It is proposed that a regulatory lite framework may be adopted for usage of AI/ML in securities market for any purpose other than for business operations that may directly impact their customers/clients (Indicative list specified at para 5.2 (a)). For instance, for usage of AI/ML by SEBI regulated entities for internal compliance purpose, surveillance, advanced cyber security tools etc., only points number 5.1(a), 5.1(f), 5.1(i), 5.1(n), 5.3 and 5.5 as mentioned above may be made applicable for the SEBI regulated entities.

7. PUBLIC COMMENTS

7.1 SEBI invites comments, supported by rationale, from all stakeholders on the guiding principles and tiered approach outlined in this paper at para 5 and 6 above.

7.2 The comments/ suggestions maybe submitted latest by July 11, 2025 through web based online mode at the following link: -

https://www.sebi.gov.in/sebiweb/publiccommentv2/PublicCommentAction.do?doPublicComments=yes.

7.3 In case of any technical issue in submitting your comment(s) through the web based public comments form, you may email your comment(s) to Mr. Ansuman Dev Pradhan (GM) (ansumanp@sebi.gov.in) / Mr. Harshad Patil (AGM) (harshadp@sebi.gov.in). While sending the email, kindly mention the subject as “Guidelines for responsible usage of AI/ML in securities markets”

Issued on: June 20, 2025

****

Annexure A

Artificial Intelligence

The term Artificial Intelligence, first coined by data scientist John McCarthy, is defined as "the science and engineering of making intelligent machines"[5], or simply, the study of methods for making computers mimic human decisions to solve problems. AI includes tasks such as learning, reasoning, planning, perception, language understanding and robotics. As per National Strategy for AI document 2018, AI has been defined as "A constellation of technologies that enable machines to act with higher levels of intelligence and emulate the human capabilities of sense, comprehend and act".

Machine Learning

Machine Learning is a subset and application of AI, which focuses on the development of computer programs –designed to automatically learn the rules to perform a specified task by looking at data with many examples relevant to a task. A machine-learning system is trained rather than explicitly programmed.

[5] Artificial Intelligence Definitions by Stanford University PDF

Annexure B

RISK	POSSIBLE CONTROL MEASURES
A. **Malicious usage leading to market manipulation and/or misinformation**: Generative AI has the capability to create fraudulent financial statements, misleading news articles, or deepfake content, which can result in price manipulation or market instability.	1. **Watermarking and Provenance Tracking**: Integrating digital signatures into AI-generated content to help verify authenticity and detect fakes. 2. **Suspicious activity Reporting**: Market participants may be encouraged to report any suspicious AI-related activities to the regulatory authority. 3. **Public Awareness Campaigns**: Educating investors about AI-generated misinformation risks.
B. **Concentration Risk**: Reliance on a limited number of Gen AI providers (technology infrastructure / data) by market participants can lead to systemic risks in times of failure or impairment	1. **Detection and monitoring of concentration**: Market participants may be required to periodically report the names of third party vendors/service providers engaged by them for AI services. This will enable the regulator to monitor any build-up of concentration. 2. **Diversification of Providers**: Encourage use of multiple AI suppliers. 3. **Enhanced monitoring of critical vendors and of AI applications provided by them:** Any dominant providers of AI systems / models to the financial markets may be designated as critical service providers and AI applications of such providers used by market participants be subject to enhanced monitoring such as more frequent reporting

	of performance results and audit findings. Such critical AI vendors can also be monitored for resilience.
C. **Herding and Collusive Behaviour**: Widespread use of common models and datasets may have potential impacts on financial markets, in particular if these models and datasets are used in similar ways by systemically important institutions or by large cohorts of market participants	1. **Diverse AI Models and Data Sources**: Promote usage of varied AI architectures and proprietary datasets by market participants. 2. **Monitoring of herding behaviour:** Stock exchanges can be mandated to monitor potential herding behaviour arising from similar AI-driven strategies. 3. **Algorithmic Auditing**: Regular audits to be conducted to detect collusive patterns. 4. **Circuit Breakers:** Implementation of circuit breakers to respond to AI-driven amplified market volatility.
D. **Lack of explainability:** Gen AI models are generally difficult to comprehend or explain how	1. **Documentation and Reporting:** Market participants can be required to maintain detailed AI process documentation.

system computes an output given a particular input. Therefore, assessing the robustness and suitability of a model for any particular use becomes difficult. This may also impede supervision and regulatory oversight.	2. **Explainable AI Requirements:** Use of interpretable AI models or explainability tools which can explain working of AI model. 3. **Human Oversight:** Mandate human review of AI outputs.
E. **Model failure / runaway AI behaviour:** Flaws in Gen AI systems could spread across markets, potentially leading to financial instability.	1. **Stress Testing:** To assess the AI performance, extreme scenarios to be simulated to do stress testing. 2. **Volatility Controls:** Implement circuit breakers and kill switches. 3. **Human oversight and accountability:** To prevent over-reliance on AI systems, market participants can implement human-in-the-loop or human-around–the-loop mechanisms. Further, AI governance structure should provide for human accountability for AI-driven decisions.
F. **Lack of Accountability and Regulatory Non-Compliance:** AI system usage may lead to compliance lapses, regulatory	1. **Regulatory Sandboxes**: AI systems can undergo thorough testing in controlled environments to ensure they do not result in regulatory breaches. 2. **Human oversight and accountability:** To prevent over-reliance on AI systems, market participants can implement human-in-the-loop or human-around–the-loop mechanisms.

infractions, and investor losses, particularly if their outputs are not effectively monitored. Moreover, market participants might attempt to avoid liability for such outcomes by attributing them to the AI systems.	Further, AI governance structure should provide for human accountability for AI-driven decisions. 3. **Training and Awareness**: Training of staff on the potential compliance risks associated with the use of AI.

****