Bridging innovation and compliance

Machine learning models in Financial Crime Compliance (FCC)

November 2025

KPMG. Make the Difference.

Contents

1 Introduction

Confronted by the surge in sophisticated financial crime and rising customer expectations, banking industry stand at a **'to be or not to be'** philosophy[1] for adopting Artificial Intelligence (AI) model. This adoption may no longer be optional—it's existential. Legacy systems relying on static rules and manual reviews are progressively losing effectiveness against modern fraud. Tools such as **MuleHunter.ai,** developed by RBI Innovation Hub, are now being implemented by over 15 Indian banks, with **95 per cent accuracy** reported by one of major bank in detecting mule accounts[2]. These models are not just upgrades—they're survival strategies.

- As per 2025 World Economic Forum white paper[3]**, financial services have spent ~ USD35 billion on AI till 2023,** with projected investments across banking, insurance, capital markets and payment business expected to reach **USD97 billion by 2027.**

- The **GenAI** segment alone is forecast to cross **~ USD12 billion by 2033** and is poised to improve banking operations in India by upto **46 per cent[4].** Further, a recent market survey highlighted that Indian financial sector's AI adoption is accelerating with over **80 per cent** of financial institutions using it for **chatbots and virtual assistants,** while **65 per cent** respondents adopted for **fraud detection[5].**

RBI's FREE-AI framework and SEBI's guidelines are set to shape responsible innovation, while initiatives like IndiaAI Mission[6] provide infrastructure and funding support. Financial institutions are moving from pilot projects to full-scale machine learning integration, using models for AML, fraud detection, and customer personalisation.
We have set out strategic and technical imperatives of machine learning adoption in financial crime compliance with focus on banking sector.

[1] To be, or not to be: that is the question; Shakespeare's Hamlet
[2] RBI's fraud detection tool MuleHunter AI expands reach with over 15 more banks nearing rollout; Moneycontrol; August 2025
[3] Artificial Intelligence in Financial Services; World Economic Forum; January 2025
[4] FREE-AI Committee Report – Framework for Responsible and Ethical Enablement of Artificial Intelligence; Reserve Bank of India; August 2025
[5] Account Aggregators to connect underserved segments with financial sector: NITI Aayog; Press release by FICCI, February 2022
[6] IndiaAI Mission; Website of IndiaAI

2 Model usage across customer lifecycle

In the banking sector, the customer lifecycle spans across multiple stages, each presenting unique risks and opportunities. At every stage, banks can leverage AI models to enhance decision-making, improve customer experience, and strengthen financial crime surveillance. The following section highlights various types of models and their indicative usage across different phases of the customer journey.

Figure 1: Indicative models

M1 Neural network

Uses interconnected layers of nodes to find complex, non-linear patterns in data and make predictions.

Supervised learning model

M2 Logistic regression

Used for predicting a categorical outcome by calculating the probability of a data point belonging to a certain class.

Supervised learning model

M3 Decision trees

Uses a tree-like structure to make predictions by splitting the data into branches based on a series of simple if-then-else rules.

Supervised learning model

M4 Random forest

Combines the predictions from multiple independent decision trees to improve overall accuracy and reduce the risk of overfitting.

Supervised learning model

M5 Gradient boosting

Sequentially builds multiple weak models, with each new model trained to correct the prediction errors made by the previous ones.

Supervised learning model

🟦 Supervised methods are generally used for identifying known patterns, basis the target labels defined within historical datasets.

M6 K-means clustering

Groups unlabeled data into pre-specified number of clusters (k) by iteratively assigning each data point to the cluster with nearest mean.

Unsupervised learning model

M7 Hierarchical clustering

Builds a hierarchy of clusters by either merging small clusters into larger ones or by recursively splitting a large cluster into smaller ones.

Unsupervised learning model

M8 Isolation forest

Identifies outliers by randomly selecting and partitioning data points until anomalies are isolated, making it efficient for large datasets

Unsupervised learning model

🟪 Unsupervised methods are generally used for identifying unknown risks and emerging typologies.

Following is an indicative list of use cases of models currently being used widely across each stage of customer lifecycle:

Table 1: Indicative use of models

Stage	Indicative use case	M1	M2	M3	M4	M5	M6	M7	M8
I. Customer sourcing, profiling, and lead management	a. Data farming and linkage analysis	■	□	□	□	□	■	■	□
	b. Predictive and behavioural analytics	□	□	□	□	□	■	■	□
	c. Lead management.	□	□	□	■	□	□	□	□
II. Customer onboarding and due diligence	a. Customer onboarding	□	■	□	□	□	□	□	□
	b. Customer due diligence	□	■	■	■	■	□	□	□
	c. Enhanced due diligence	■	■	■	□	□	□	□	□
	d. Sanction screening.	□	■	□	□	□	□	□	□
III. Risk assessment and regulatory reporting	a. Customer risk rating	□	■	■	□	□	□	□	□
	b. Monitoring suspicious activities	■	□	□	■	■	□	□	■
	c. Network/linkage analytics	■	□	□	□	□	□	□	□
	d. Reporting processes (SAR/STR).	□	■	□	■	■	□	□	□
IV. Customer experience	a. Customer grievance management	□	□	■	□	□	□	□	□
	b. Data driven root cause analysis	□	□	■	□	□	□	□	□
	c. Chatbots and virtual assistants.	■	□	■	□	□	□	□	□

Recent RBI report[7] highlights increased adoption of AI tools by banks for Financial Crime Compliance (FCC), wherein out of total 583 AI tools being used/planned to be used across surveyed entities[8], 101 AI tools were being utilised for FCC area (Fraud detection, AML/CFT/KYC and Early Warning Signals). Regulatory landscape for this area has also evolved with enhancements in Master Direction on Fraud Risk Management (2024) wherein FIs are encouraged to develop AI driven fraud detection mechanism under Chapter III "Framework for Early Warning Signals for detection of fraud" and regularly test these models for accuracy and bias in fraud detection.

□ □ Can be used basis format of data

■ ■ Widely used

[7] FREE-AI Committee Report – Framework for Responsible and Ethical Enablement of Artificial Intelligence; Reserve Bank of India; August 2025

[8] These comprises of Scheduled Commercial Banks (SCBs), Urban Co-operative Banks (UCBs), Non-Banking Financial Institutions (NBFCs), ARCs and AIFIs

3 Crucial role and regulatory scrutiny on financial crime compliance

FCC is a cornerstone function for banks, encompassing a broad range of services designed to uphold the integrity of financial system and prevent its exploitation for illicit purposes. At the very heart of FCC lies **Anti-Money Laundering (AML)**, a critical pillar dedicated to detecting and preventing the process by which illegally obtained funds are disguised as legitimate income. It involves a structured approach to detect and prevent the movement of illicit funds through financial systems. Further, role of FCC is **transitioning from transaction monitoring to Monitoring of Suspicious Activities (MSA)**, wherein customer behaviour and attributes are also considered along with transactions for flagging potential suspicious activities[9]. Thus, the global fight against financial crime hinges on robust AML frameworks, preventing funds from financing terrorism, drug trafficking, and other grave offenses that destabilise economies and societies.

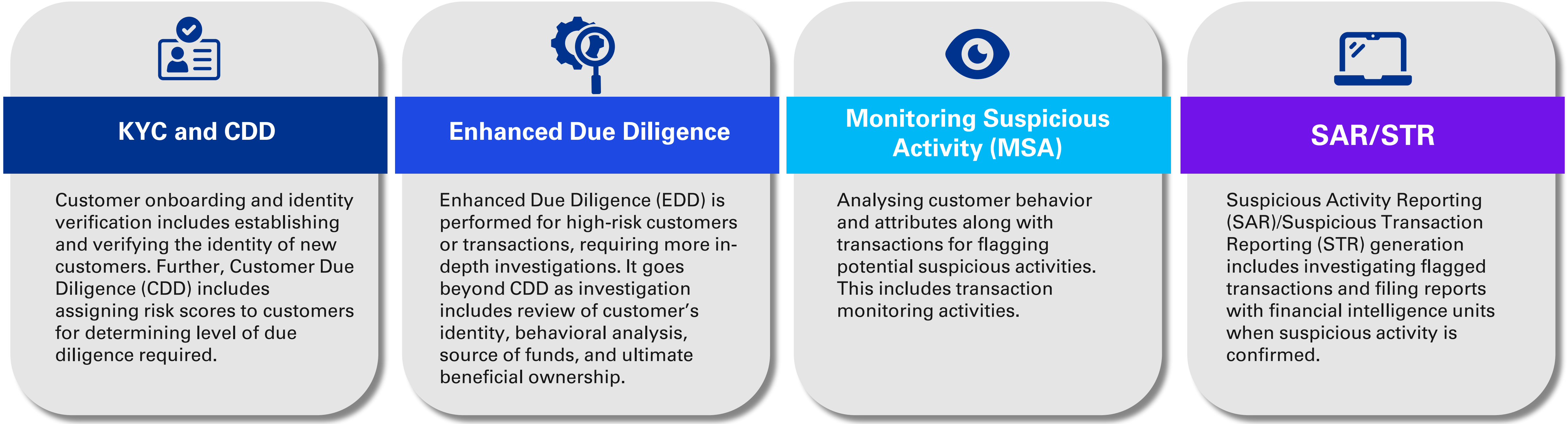
The importance of AML measures is consistently emphasised by global forums, regulators, and international organisations. In recent times, there has been a significant intensification of regulatory scrutiny and enforcement, leading to **substantial penalties** towards major financial institutions **for AML control weaknesses**[10] and **AML compliance failures** (including weaknesses in transaction monitoring systems)[11]. These cases convey a critical regulatory message: AML compliance is not merely a box-ticking exercise but a fundamental obligation, and failures may have severe and financially impactful consequences. Regulators expect banks to leverage advanced capabilities to keep pace with the increasingly sophisticated methods employed by illicit actors.

[9] The Wolfsberg Statement on Effective Monitoring for Suspicious Activity, Part II: Transitioning to Innovation; The Wolfsberg Group; August 2025
[10] FCA fines £29m for failings in financial crime systems and controls; Financial Conduct Authority; October 2024
[11] Bank fined $3bn in historic money laundering settlement ; BBC; October 2024

4 Limitations of current manual/rule-based practices

Within AML, banks engage in a variety of critical activities, including:

Figure 2: Activities involved in AML



KYC and CDD

Customer onboarding and identity verification includes establishing and verifying the identity of new customers. Further, Customer Due Diligence (CDD) includes assigning risk scores to customers for determining level of due diligence required.

Enhanced Due Diligence

Enhanced Due Diligence (EDD) is performed for high-risk customers or transactions, requiring more in-depth investigations. It goes beyond CDD as investigation includes review of customer's identity, behavioral analysis, source of funds, and ultimate beneficial ownership.

Monitoring Suspicious Activity (MSA)

Analysing customer behavior and attributes along with transactions for flagging potential suspicious activities. This includes transaction monitoring activities.

SAR/STR

Suspicious Activity Reporting (SAR)/Suspicious Transaction Reporting (STR) generation includes investigating flagged transactions and filing reports with financial intelligence units when suspicious activity is confirmed.

Historically, the abovementioned activities have been predominantly carried out either manually – relying on human analysts to meticulously review data and spot anomalies – or through rule-based systems. While rule-based systems offered an initial step towards automation by setting predefined thresholds and conditions, they suffer from significant inherent limitations:

Figure 3: Limitations of rule-based systems

1

High false positive rates

These systems often generate a large number of false alerts, flagging legitimate transactions as suspicious, which creates substantial investigative backlogs for compliance teams.

2

Limited pattern recognition

They can only identify patterns explicitly programmed into them, failing to detect complex, multi-variable relationships or subtle anomalies indicative of sophisticated schemes.

3

Rigidity and lack of adaptability

Rule-based systems are static and struggle to adapt to new and evolving money laundering typologies. Criminals constantly devise new methods, and updating rules manually is a slow, reactive process.

4

Scalability challenges

The sheer volume of transactions in modern banking makes manual review or even managing an extensive rule-set increasingly impractical and cost-prohibitive. Analysts are often overwhelmed, leading to potential oversight of genuine threats.

5 Usage of models for solving current challenges

Machine learning models are emerging as transformative solutions, offering a powerful paradigm shift in how AML measures are undertaken. By leveraging advanced algorithms and computational power, these models can address the fundamental limitations of existing processes and offer numerous advantages:

- **Enhanced detection and accuracy**: Models can uncover hidden patterns and anomalies in large datasets, reducing false positives and improving compliance focus
- **Adaptive learning and evolving threat detection**: ML systems evolve with new data, identifying emerging money laundering tactics and staying ahead of criminal innovation
- **Real-time monitoring and proactive intervention:** AI enables near-instant transaction analysis, allowing swift action to disrupt suspicious activities before damage occurs
- **Improved efficiency and automation:** Routine tasks like alert generation and SAR drafting are automated, freeing analysts for deeper investigations and strategy
- **Better risk profiling and customer segmentation:** AI builds dynamic risk profiles using behavioural and external data, enabling tailored due diligence and segmentation
- **Scalability:** AI systems scale effortlessly with growing data volumes, supporting global operations without added human resources.

6 Model-driven usage for specific AML activities

The summary and details of indicative models and techniques which can be used for different AML activities, leveraging their unique strengths to address specific challenges, are as below:

Figure 4: Models used for different AML activities

KYC and CDD

- Natural Language Processing (NLP)
- Machine learning classification models
- Computer vision (for digital KYC).

Enhanced Due Diligence

- Machine learning models
- Network analysis (graph databases and algorithms)
- Natural Language Processing (NLP).

Monitoring Suspicious Activity (MSA)

- Unsupervised learning models (anomaly detection)
- Supervised learning models
- Behavioral analytics.

SAR/STR

- Machine learning models
- Natural Language Processing (NLP)/Generative AI

A. **Know Your Customer (KYC) and Customer Due Diligence (CDD):** This process includes verification of customer's identity, financial profile and determining the risk level for financial transactions. Following indicative models can be utilised for this process:

Natural Language Processing (NLP):

- Named Entity Recognition (NER) and information extraction: These algorithms can be used to rapidly **extract relevant details** from unstructured documents (like names and date of birth from identity proofs etc.)
- Text classification: These algorithms can be used to categorise documents or **classify customers** based on textual data (e.g., categorising business descriptions to assess industry risk).

Computer vision (for digital KYC):

- Facial recognition and liveness detection: These models can be used to **verify customer's identity against official documents** and prevent fraud during digital onboarding
- Optical Character Recognition (OCR): These algorithms can be used **to extract data from physical documents** (e.g., passports, utility bills) quickly and accurately.

Machine learning classification models:

- Logistic regression, decision trees, random forests or Gradient Boosting Machines (GBMs): These algorithms can be used to predict customer risk scores based on collected demographic data, occupation, geographic risk factors, and adverse media findings. These models can weigh different risk indicators to provide an extensive score.

B. **Enhanced Due Diligence (EDD):** EDD is a set of measures designed to assess customers based on their risk profiles. It plays a crucial role in dealing with high-risk customers. Following indicative models can be utilised for this process.

Natural Language Processing (NLP):

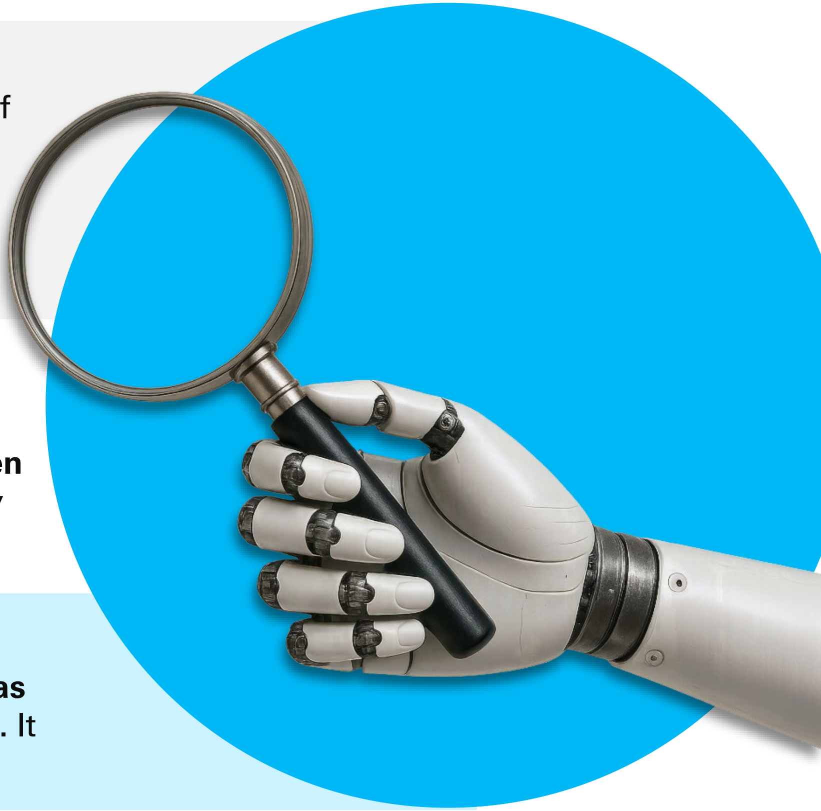
- Information extraction and text summarisation: These models can rapidly sift through large volumes of unstructured data (e.g., legal documents, company filings, news reports, court records) to **extract key information** about individuals, companies, and their activities, and to **summarise findings** for analysts
- Semantic search: These algorithms can be used to **intelligently search vast databases for relevant information** during complex investigations.

Network analysis (graph databases and algorithms):

- Graph Neural Networks (GNNs) or traditional graph algorithms (e.g., PageRank, centrality measure: These algorithms can be used for **mapping complex beneficial ownership structures, identifying hidden relationships** between individuals and entities, and uncovering money mules or shell companies. They can analyse interconnected financial networks to find patterns of collusion or control.

Machine learning models:

- Logistic regression or decision trees: These models can be used to **classify customers or transactions as high-risk or low-risk** based on various features like geography, transaction volume, and customer type. It calculates the probability of a customer being high-risk and assigns a risk score.



C. **Monitoring Suspicious Activities (MSA):** It is the process of tracking and analysing customer behaviour and attributes along with financial transactions to identify suspicious activity, ensure regulatory compliance, and prevent financial crimes like money laundering, fraud, and terrorist financing. Following indicative models can be utilised for this process:

Unsupervised learning models (anomaly detection):

- Isolation forest: This algorithm is effective at identifying outliers in high-dimensional datasets. It works by isolating anomalies rather than profiling normal data
- One-class SVM (Support Vector Machine): This algorithm identifies anomaly by creating a boundary around 'normal' data points and flagging anything outside this boundary as an outlier
- Clustering algorithms (e.g., K-Means, DBSCAN): This algorithm groups similar transactions or customer behaviours together and identifies outliers which appears as small, isolated clusters or data points far from any cluster centroid.

Supervised learning models:

- Random forests/Gradient Boosting Machines (GBMs): This algorithm is generally used for **classification tasks,** which are trained on historical data labelled as 'suspicious' or 'legitimate'. These algorithms can be used to identify **complex non-linear relationships**
- Neural networks (e.g., LSTMs for sequential data): These supervised algorithms are generally used for **identifying patterns in sequential transaction data** (e.g., unusual sequences of deposits and withdrawals, or rapid movement of funds across multiple accounts). Recurrent Neural Networks (RNNs) like LSTMs can learn from the temporal aspect of transactions, thus making it more reliable for **time series forecasting and speech recognition.**

Behavioural analytics:

- It can be used for conducting behavioural analysis by establishing dynamic baselines for individual customer behaviour (spending habits, transaction types, geographic locations) and flagging deviations from these personalised norms.

D. Suspicious Activity Reporting (SAR)/Suspicious Transaction Reporting (STR):

These reports enable financial institutions to alert regulators on potentially illegal activities. Machine learning models can assist in generating these reports by detecting anomalies and streamlining initial analysis, though final judgment remains human-led. In addition to the models used for MSA, following indicative models can be utilised for this process:

Machine learning models:

- Logistic regression: This **algorithm classifies transactions or customer behaviors as potentially suspicious** based on historical patterns. It analyses features such as transaction amount, frequency, customer risk profile, and geographic indicators to estimate the probability of suspicious activity
- Random forest and XGBoost: These models analyse large volumes of transaction and customer data to **identify complex, non-linear patterns that may indicate financial crime.** Random Forest builds multiple decision trees and aggregates their outputs to improve accuracy and reduce false positives, while XGBoost uses gradient boosting to sequentially refine predictions, making it highly effective for dynamic risk scoring.

Natural Language Processing (NLP)/Generative AI (GenAI):

- Text generation models (e.g., transformer-based models like GPT): These models can be used to **draft initial SAR narratives** by summarising key findings from structured data (like transactions, customer profiles, etc.) and unstructured investigation notes. This can significantly reduce manual effort in compiling narrative sections
- Sentiment analysis and topic modelling: These algorithms can be used to understand the context and key insights from investigator notes and external intelligence and **flagging adverse points** for customers. This streamlines the process and significantly reduces manual efforts.

By strategically deploying these diverse models across various AML activities, banks can move towards a more intelligent, efficient, and proactive defence against financial crime.

7 Risk landscape

The Financial Stability Board (FSB)[12] has highlighted that increased adoption of AI technologies can amplify **systemic vulnerabilities**—such as market correlations and operational dependencies. For instance, AI models trained on historical data may reinforce procyclicality, intensifying boom-bust cycles. Excessive reliance on similar algorithms across institutions can lead to model convergence, reducing market diversity and resilience. Moreover, AI systems may behave unpredictably under rare or extreme conditions.

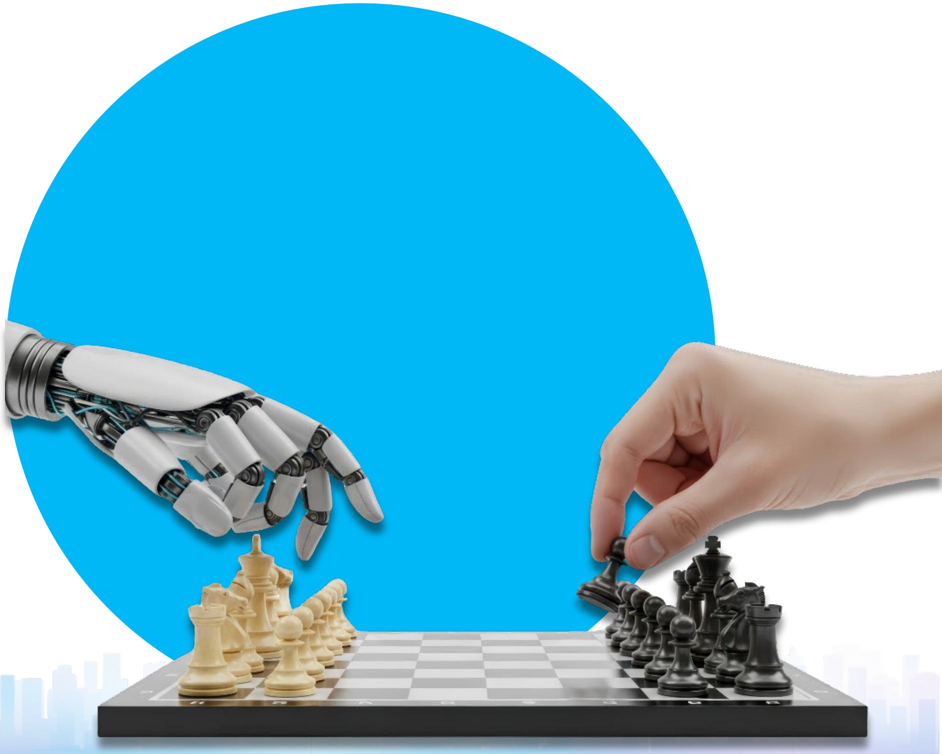
The 2010 Flash Crash[13] serves as a stark reminder of how automated systems, if not adequately stress-tested, can trigger severe market disruptions (in 2010 flash crash automated trading algorithms contributed to a rapid and severe market downturn, erasing nearly USD1 trillion in market value within minutes).

RBI in its publication[14] highlighted various risk factors associated with adoption of model in financial service. Key risks factors are as below:

- **Opaque decision-making (‘black box’ problem):** Many AI models, especially deep learning systems, lack transparency. Their decisions are difficult to interpret, making it challenging for institutions to justify outcomes to regulators or customers
- **Data poisoning and input manipulation**: AI systems are vulnerable to adversarial attacks where malicious actors subtly alter training data. For example, poisoning transaction data used in fraud detection could cause the model to misclassify fraudulent behaviour as legitimate

[12] The Financial Stability Implications of Artificial Intelligence; Financial Stability Board; November 2024
[13] Selling Spirals: Avoiding an AI Flash Crash; Lawfare; November 2024
[14] FREE-AI Committee Report – Framework for Responsible and Ethical Enablement of Artificial Intelligence; Reserve Bank of India; August 2025

- **Bias and unequal access:** AI models can unintentionally reinforce societal biases, especially when trained on skewed datasets. This can widen the financial access gap, particularly in underserved regions where alternative credit scoring is used
- **Operational and infrastructure vulnerabilities**: AI introduces new risks at multiple levels—model, data, and infrastructure. These include cybersecurity threats, model drift, and performance degradation over time
- **Limited monitoring and governance practices:** Despite growing adoption, many institutions lack robust monitoring frameworks. Few use tools like SHAP or LIME for explainability, and real-time performance tracking remains rare. As per a recent market survey conducted by regulators[15], it was observed that only 15 per cent of respondents were using interpretation tools like SHAP or LIME for explainability while only 35 per cent were validating for biasness and fairness checks (*which were also limited to development stage and not extended to deployment stages*)
- **Talent and resource constraints:** Barriers such as the AI talent gap, high implementation costs, and limited access to quality data and computing power continue to hinder responsible AI deployment.



[15] FREE-AI Committee Report – Framework for Responsible and Ethical Enablement of Artificial Intelligence; Reserve Bank of India; August 2025

To address these risks, regulators are increasingly advocating for structured governance and independent validation. **The RBI's FREE-AI Framework** provides a comprehensive roadmap for responsible AI adoption in India's financial sector:

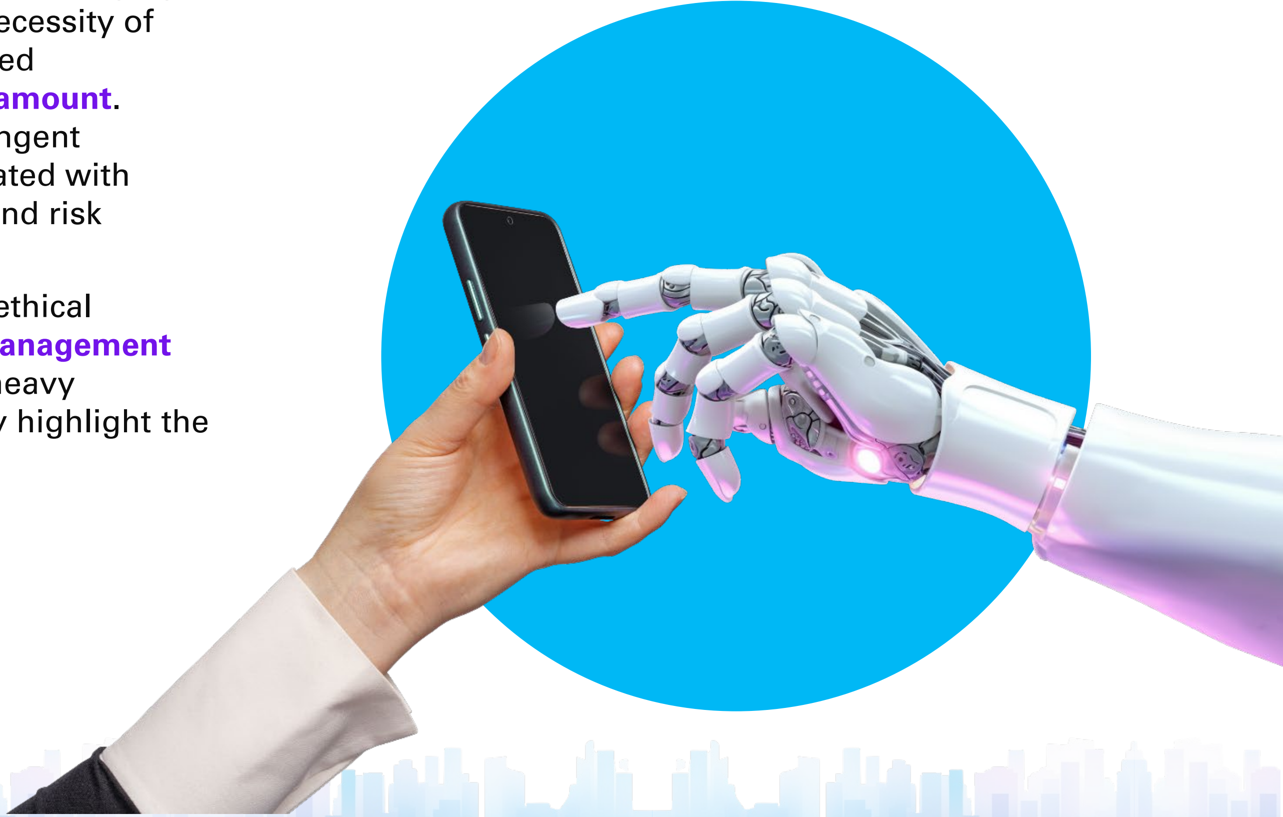
- **Board approved AI policies:** Institutions must formalise AI governance through board-level oversight. Further, Risk Management Committee and AI Adoption Committee may be formed for integrating AI-related risk with overall risk management framework and ensuring that AI innovation/adoption are cross departmental and well managed
- **Expanded risk and audit protocols:** Product approvals, consumer protection, and cybersecurity frameworks should include AI-specific considerations
- **Lifecycle governance:** From development to deployment, AI systems must be governed with clear accountability and transparency
- **Consumer awareness:** Customers should be informed when interacting with AI systems
- **Incident reporting and graded supervision:** A risk-based approach to supervisory action encourages innovation while ensuring accountability. Institutions demonstrating proactive remediation may be given leeway, while repeated failures could trigger penalties.

Additionally, **industry-developed toolkits** such as those by Infosys, NASSCOM, IBM, and Microsoft offer technical guardrails for bias detection, performance monitoring, and ethical deployment.

8 The imperative of independent model validation

While the power of machine learning models in AML framework is undeniable, leveraging these sophisticated models comes with a critical responsibility: the absolute necessity of independent validation. Given the potential 'black box' nature of some advanced algorithms, ensuring their **accuracy, fairness, reliability, and robustness is paramount**. Independent validation is not merely a leading practice; it is increasingly a stringent regulatory requirement. Regulatory bodies recognise the inherent risks associated with reliance on complex, data-driven models for critical financial crime detection and risk management decisions.

This is precisely why RBI has recommended a framework for responsible and ethical enablement of AI in financial sector, and guidelines like **SS 1/23 (model risk management principles for banks)** issued by Prudential Regulation Authority (PRA) place a heavy emphasis on **robust model risk management**. These regulations unequivocally highlight the importance of validation requirements[16].

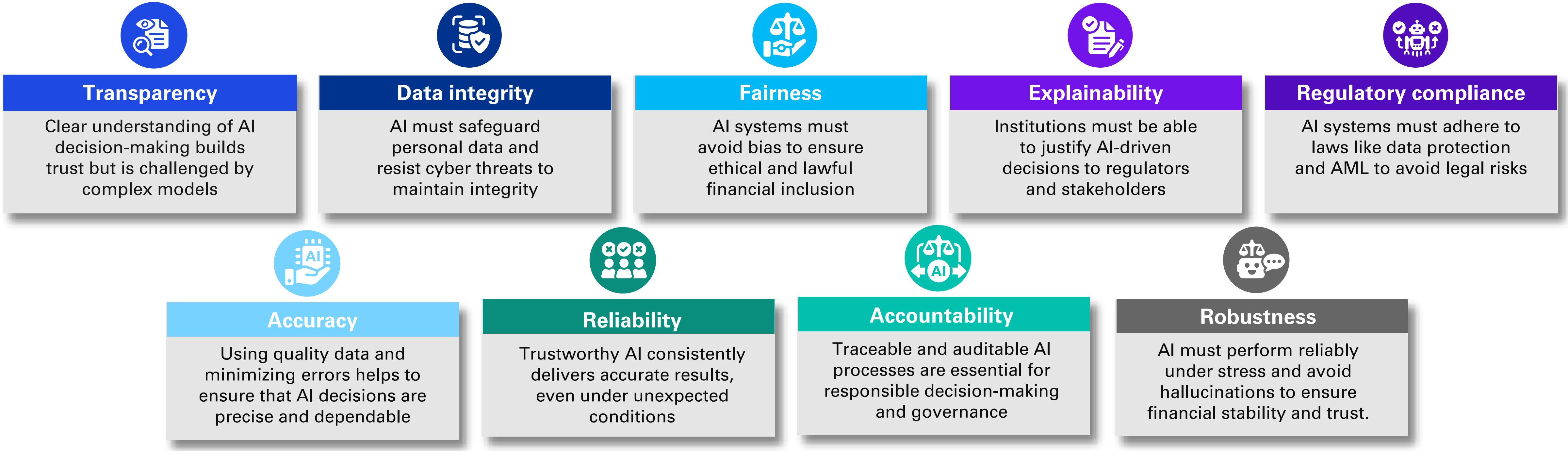


[16] Basis the AI system governance framework (Recommendation No. 16 of FREE AI-Framework), RBI has recommended banks to conduct regular model validation and ongoing monitoring activities for ensuring safe usage of the models. Additionally, Principle 4 of SS 1/23 guidelines lay emphasis on independent model validation activities.

The deputy governor of Reserve Bank of India (RBI)[17] and Monetary Authority of Singapore (MAS)[18] have recommended general FEAT principles in lines with principles and practices of 'Responsible AI' which financial institutions may consider while designing AI solutions in order to strike a balance between innovation and responsible use of technology. Summary of these key principles are as below:

Key principles for 'Responsible AI'

Figure 5: Key principles of Responsible AI



Transparency
Clear understanding of AI decision-making builds trust but is challenged by complex models

Data integrity
AI must safeguard personal data and resist cyber threats to maintain integrity

Fairness
AI systems must avoid bias to ensure ethical and lawful financial inclusion

Explainability
Institutions must be able to justify AI-driven decisions to regulators and stakeholders

Regulatory compliance
AI systems must adhere to laws like data protection and AML to avoid legal risks

Accuracy
Using quality data and minimizing errors helps to ensure that AI decisions are precise and dependable

Reliability
Trustworthy AI consistently delivers accurate results, even under unexpected conditions

Accountability
Traceable and auditable AI processes are essential for responsible decision-making and governance

Robustness
AI must perform reliably under stress and avoid hallucinations to ensure financial stability and trust.

These guidelines underscore that model validation is essential for building trust in AI systems, mitigating potential errors or biases, and help ensuring regulatory compliance.

[17] FREE-AI Committee Report – Framework for Responsible and Ethical Enablement of Artificial Intelligence; Reserve Bank of India; August 2025

[18] Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector; Monetary Authority of Singapore

Key consideration during model validation for FCC models

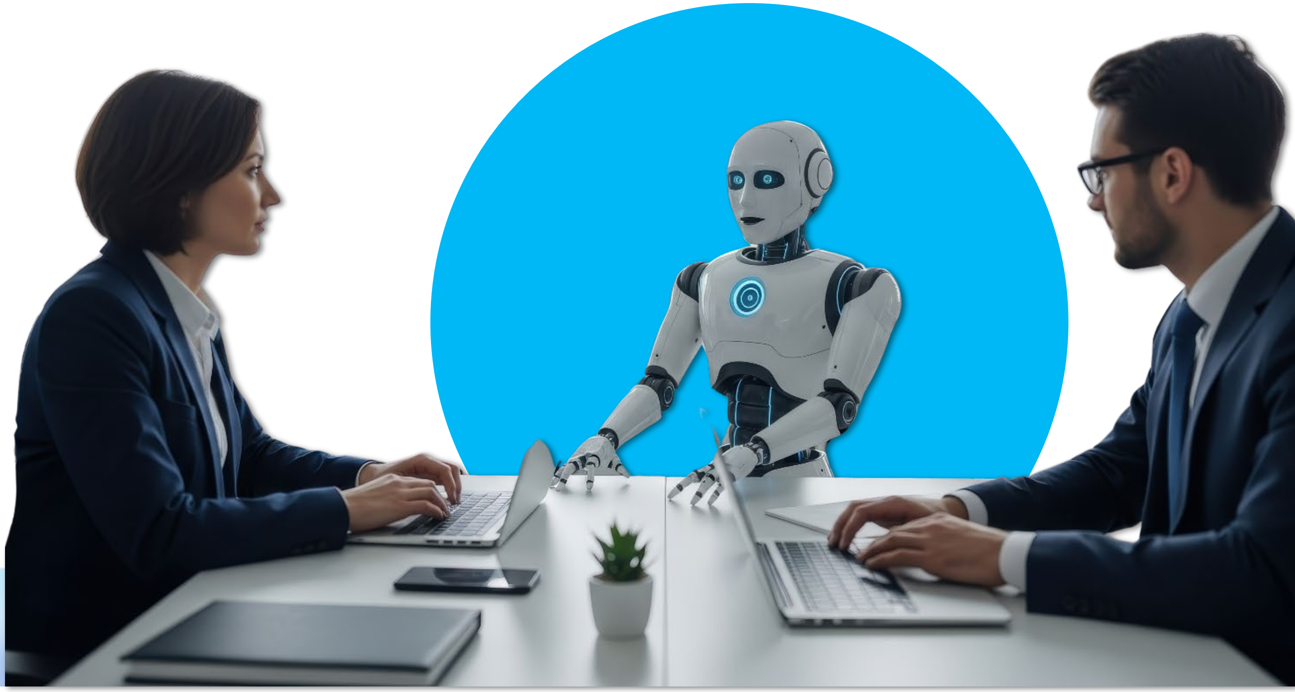
As financial institutions increasingly deploy models for Financial Crime Compliance (FCC), model validation must evolve to reflect the unique risk dynamics of this domain. Unlike prudential models, FCC models require a nuanced balance between **model risk**—the potential for inaccurate or biased outputs—and **financial crime risk**—the threat of undetected illicit activity. Independent validators must assess whether the risk of deploying a sub-optimal model is outweighed by the risk of not deploying a model that could enhance detection capabilities.

Financial institutions should evolve from basic 'drag-net' and 'catch-all'[19] dependency approach, which are often ineffective and leads to lower quality of reporting. Further, validation should not be limited to historical pattern recognition; it must also evaluate the model's ability to detect emerging fraud typologies and adapt to evolving threats. This calls for hybrid approaches combining supervised and unsupervised techniques. To avoid delays, institutions should adopt agile validation frameworks—validating core models rigorously while streamlining sub-model assessments based on scope and delta changes.

Lastly, **explainability** remains a cornerstone of trust and oversight. Validators must ensure transparency across the model lifecycle:

- Risk coverage (mapping features to typologies)
- Model design and calibration (clarity on data, algorithms, and training)
- Model usage (interpretability for investigators and decision-makers).

These considerations are essential for aligning model governance with the institution's risk appetite and regulatory expectations, while enabling timely innovation in FCC.

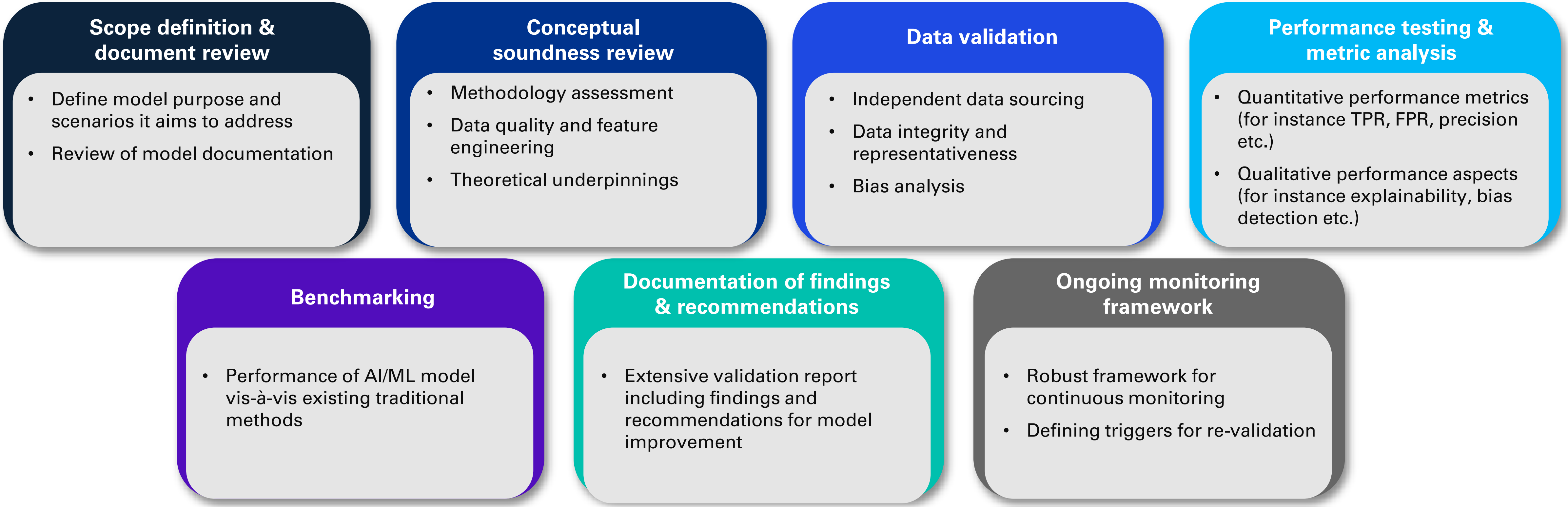


[19] 'Drag net' approach and 'Catch-all' dependency approach refer to a extensive and indiscriminate method of surveillance or monitoring, wherein a centralised platform is configured to capture and analyse the available data across systems, regardless of its initial relevance or risk profile.

9 Independent model validation procedure and key metrics

The independent validation procedure for models is a rigorous, multi-faceted process designed to thoroughly assess a model's effectiveness, reliability, and compliance. It typically involves several key steps and employs various metrics:

Figure 6: Key factors involved in independent model validation



Scope definition & document review

- Define model purpose and scenarios it aims to address
- Review of model documentation

Conceptual soundness review

- Methodology assessment
- Data quality and feature engineering
- Theoretical underpinnings

Data validation

- Independent data sourcing
- Data integrity and representativeness
- Bias analysis

Performance testing & metric analysis

- Quantitative performance metrics (for instance TPR, FPR, precision etc.)
- Qualitative performance aspects (for instance explainability, bias detection etc.)

Benchmarking

- Performance of AI/ML model vis-à-vis existing traditional methods

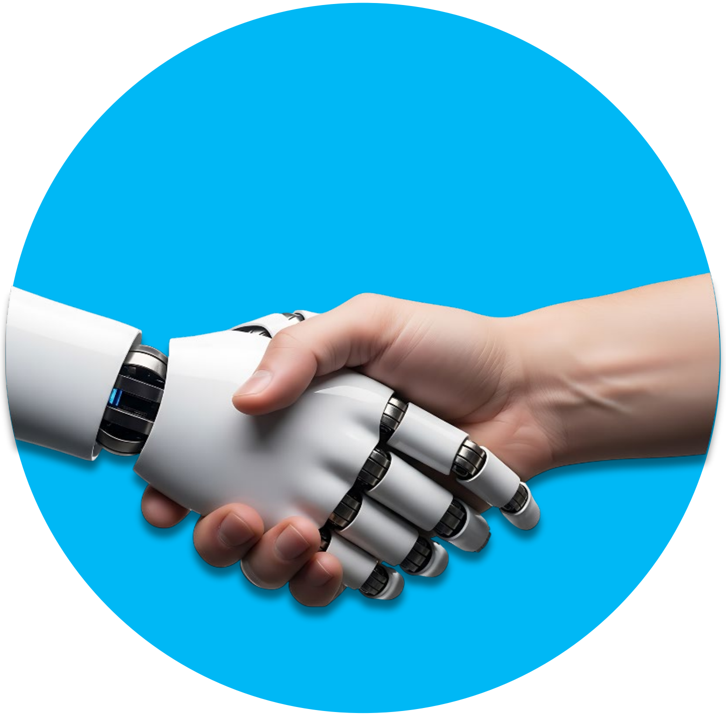
Documentation of findings & recommendations

- Extensive validation report including findings and recommendations for model improvement

Ongoing monitoring framework

- Robust framework for continuous monitoring
- Defining triggers for re-validation

- **Scope definition and documentation review:** Clearly defining the model's purpose, intended use, and specific AML scenarios it aims to address (e.g., transaction monitoring, customer segmentation)
- **Conceptual soundness review**: This includes evaluation of appropriateness and robustness of the chosen algorithms along with assessment of quality, completeness, relevance, and representativeness of the data used for model training and testing
- **Data validation:** Utilising independent datasets for validation to ensure unbiased performance assessment. This includes verifying the integrity, accuracy, completeness, and representativeness of the validation data along with checking presence of any inherent bias. Additionally, validators should assess holistic risk identification process of business for identification of potential exposure to idiosyncratic risks[20] as well as trends and emerging threats across the enterprise
- **Benchmarking:** Comparing model's performance against existing traditional methods or against industry benchmarks to quantify the incremental value and improvement
- **Documentation of validation findings and recommendations**: Compiling a comprehensive validation report detailing the methodology, findings, limitations, and recommendations for model improvement, usage, and ongoing monitoring
- **Ongoing monitoring framework**: Establishing a robust framework for continuous monitoring of the model's performance in production and defining triggers for re-validation or recalibration.



[20] Such risks would include undetected, large-scale risks (e.g. laundromats, mirror trading schemes, money mule networks). Using lessons learned from such risks detected in the past and the economic and geo-political factors which have led to these, as well as the results from its annual financial crime risk assessments, FIs would need to develop and execute “stress tests” to identify potential anomalies not identifiable through the ongoing monitoring of individual customer relationships (Source - Wolfsberg MSA I.)

Performance testing and metric analysis:

- **Quantitative performance metrics**: Rigorously evaluating the model's predictive power against pre-defined thresholds and business objectives. Key indicative metrics include:

Table 2: Indicative metrics

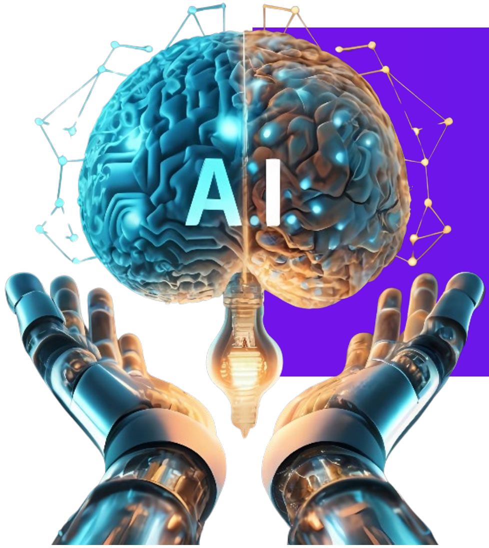
#	Evaluation metric	Usage and indications
1	Accuracy ratio	• Used for assessment of model efficiency and effectiveness • **Higher accuracy ratio** is considered better.
2	Precision	• Assists in understanding reliability of the model • **Higher precision rate** is considered better.
3	Recall	• Helps to measure ability of model to generate alerts • **Higher recall rate** is considered better.
4	F1 score	• Used to evaluate the performance of classification model by combining precision and recall • **Higher F1 score** is considered better.
5	Confusion matrix	• Helps in creating a tabular layout to visualise the performance of an algorithm.
6	AUC_ROC	• Used to assess the ability of model to distinguish between two classes • **Higher AUC score** is considered better
7	False Positive Rate (FPR)	• Assists in evaluating model efficiency • **Lower FPR** is considered better.
8	Above The Line (ATL) and Below The Line (BTL) testing	• Identify count of samples not correctly classified by model • **Lower count of FN and FP** during ATL and BTL testing is considered better.
9	Mean Squared Error (MSE)	• Measuring average squared difference between predicted and actual target value • **Lower MSE** indicates that prediction of model is closer to actual values, thus considered better.

- **Qualitative performance aspects:** For ensuring responsible and transparent AI deployment in financial services, institutions adopt practices such as explainability/interpretability (XAI) using techniques like LIME and SHAP to clarify predictions from complex models, aiding regulatory scrutiny. Further, additional tests can be performed for ensuring robustness and detecting biasedness in data.

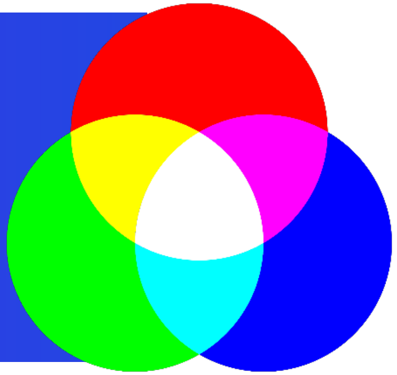
10 Conclusion: The future of AML – AI-powered and validated

Integration of AI into anti-money laundering operations represents an unparalleled opportunity for financial institutions to move beyond reactive compliance to proactive, intelligent defence against financial crime. The advantages are profound and transformative: enhanced detection capabilities, a dramatic reduction in false positives, significant increases in operational efficiency, and development of a more adaptive, resilient, and scalable AML framework that can keep pace with evolving threats.

However, realising these indicative benefits requires more than just deploying advanced technology. It necessitates a steadfast commitment to robust and independent model validation. By adhering to the stringent regulatory guidelines and by systematically validating the models, banks can ensure their cutting-edge technology is not only highly effective but also trustworthy, transparent, unbiased, and fully compliant. This dual approach – boldly embracing innovation while rigorously upholding principles of governance, oversight, and independent scrutiny – is the definitive key to truly unmasking the shadows of illicit finance and building a more secure and integrity-driven global financial system.



Financial crime like a strain of flu is constantly morphing; you may cure today's strain, but the next one evolves into something bad, if not worse. To stay ahead, FCC model management must be agile and anchored in three foundational principles: data integrity, explainability, and reliability. These are like the primary colours in the RGB spectrum - each essential on its own, and depending on the complexity of the model spectrum-based nuances can be explored. Omit one, and the framework risks breaking down at its foundation.



Acknowledgement

Our team will be happy to delve deeper into the nuances and address specific questions or challenges.

For follow-up conversations, please reach out to us by writing to Anoop Sharma by **clicking here**.

KPMG in India would like to thank

Analysis and content team:
Jai Bhandari
Samruddhi Shah
Tejas Beloskar
Dixita Bhalawat
Jaykishan Motwani
Tanmay Rane
Rishabh Modi
Aniket Nag
Nishita Khurana
Shivani Telange
Prathamesh Parab
Isha Bhattad

Design team:
Mahima

Marketing compliance team:
Nidhi Agrawal

KPMG in India contacts:

Akhilesh Tuteja
Partner and Head
Client and Markets Technology,
Media and Telecom
E: atuteja@kpmg.com

Manoj Kumar Vijai
Office Managing Partner,
Mumbai
Head - Risk Advisory
E: mkumar@kpmg.com

Rajosik Banerjee
Deputy Head – Risk Advisory
Head – Financial Risk
Management
E: rajosik@kpmg.com

Suveer Khanna
Partner and Head
Forensic Services
E: skhanna@kpmg.com

Anoop Sharma
Director
Forensic Services
E: anoopsharma@kpmg.com

kpmg.com/in

Access our latest
insights on KPMG
Insights Edge

Follow us on:
kpmg.com/in/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai – 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only/Printed in India (as per the situation).