

WHITEPAPER

## **AML 360:**

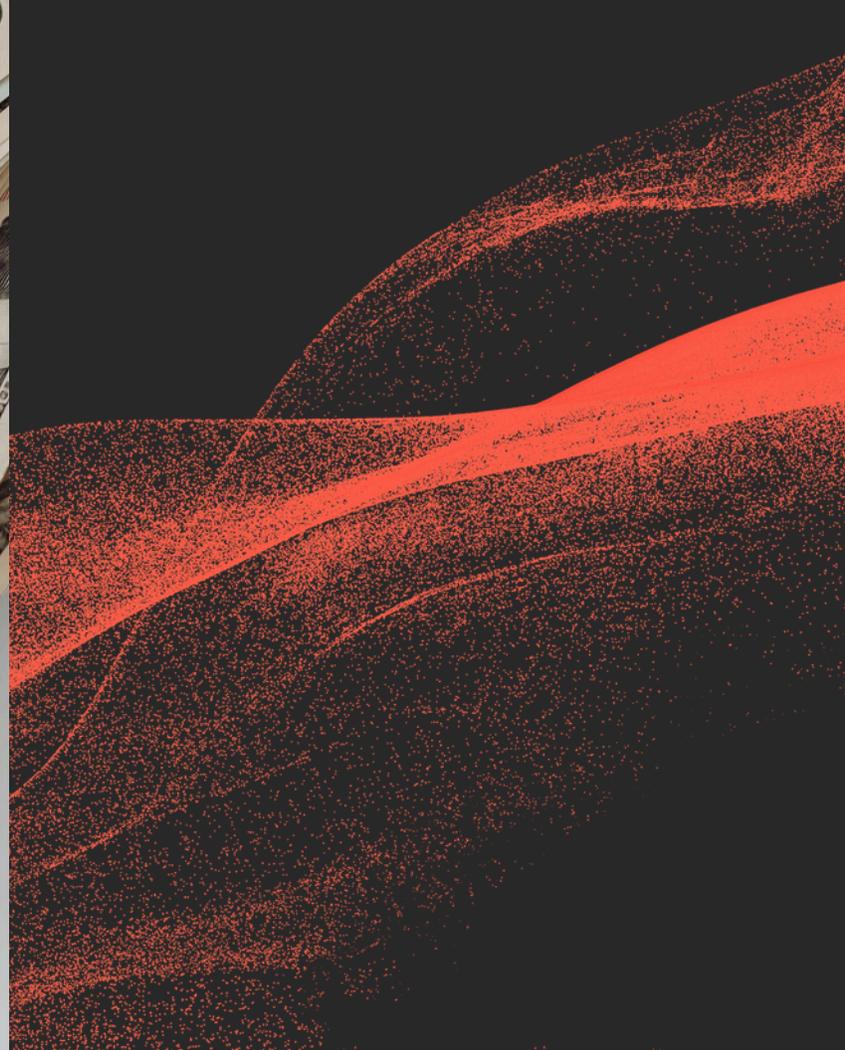
# Conversational Intelligence for Anti-Money Laundering using GenAI

Amit Sinha

Principal Enterprise Architect, LTM

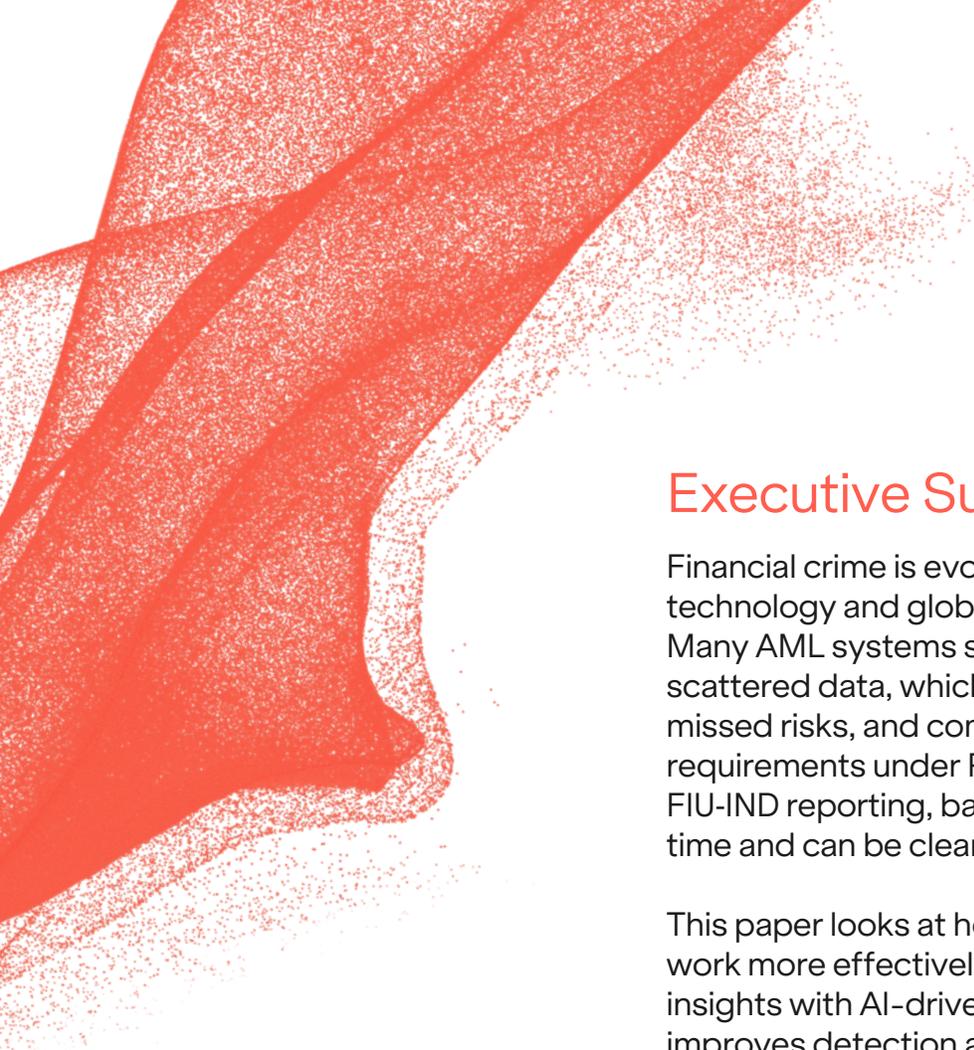
Namrata Sharma

Senior Consultant, LTM



# Table of Contents

<b>Executive Summary</b>	<b>03</b>
1.1 Market Context and AML Imperatives	
1.2 Key Benefits and Differentiators	
1.3 Indian Regulatory Landscape	
<b>Traditional Challenges for Capturing Money Laundering</b>	<b>05</b>
2.1 Graph-Based Algorithms for AML: Circular Transaction	
<b>End-to-End Conversational AML Platform: Architecture and Workflow</b>	<b>07</b>
3.1 Knowledge Graph Provides	
3.2 Challenges of LLMs	
3.3 Key Components of Solution	
3.4 Grounding Process	
3.5 Real-time Chat Interface and Uncovering Suspicious Transactions	
3.6 Automated Reporting	
<b>Strategic Roadmap for Adopting GenAI-Powered AML in Indian Banking</b>	<b>12</b>
5.1 Change Management and Adoption Challenges	
5.2 Risk, Governance, and Model Monitoring	
5.3 AML Lifecycle Coverage with GenAI	
<b>Authors</b>	<b>14</b>
<b>Appendix</b>	<b>15</b>
<b>Glossary</b>	<b>17</b>
<b>References</b>	<b>19</b>



## Executive Summary

Financial crime is evolving quickly as launderers use technology and global networks to avoid detection. Many AML systems still depend on fixed rules and scattered data, which results in too many false alerts, missed risks, and compliance issues. To meet India's requirements under PMLA, RBI's KYC guidelines, and FIU-IND reporting, banks need controls that work in real-time and can be clearly explained and audited.

This paper looks at how generative AI can help analysts work more effectively. By combining graph-based insights with AI-driven reasoning, the approach improves detection and makes regulatory reporting simpler and more reliable. The aim is to create AML operations that scale and comply with both FIU-IND and global standards.

### 1.1 Market Context and AML Imperatives

**Rising Regulatory Pressure:** Indian regulators, including FIU-IND and RBI, require banks to maintain strong monitoring systems, clear audit trails, and timely reporting through platforms like FINGate and FINnet 2.0.

**Evolving Threat Landscape:** Money laundering tactics are becoming more complex, involving layered transactions, mule accounts, and cross-border flows. Simple rule-based systems often fail to catch these patterns.

**Business Impact:** Non-compliance can lead to heavy penalties, reputational harm, and regulatory action. Banks need approaches that are risk-based and transparent.

Money laundering is becoming harder to fight as criminals use more advanced methods. Traditional AML systems are struggling to keep up with modern fraud. This paper introduces a new approach that combines generative AI with knowledge graphs to help analysts work more effectively. The solution enables natural language queries, provides context-aware detection, and automates regulatory reporting. By applying graph algorithms and large language models, banks can build AML systems that operate in real time, explain decisions clearly, and scale to meet compliance requirements under FIU-IND and global standards. The paper also outlines the technical design, key benefits, and a practical roadmap for adopting GenAI-powered AML in Indian banking.

## 1.2 Key Benefits and Differentiators

AML systems are evolving rapidly, driven by the need to uncover increasingly complex financial crime patterns. Modern, AI-enhanced AML combines contextual intelligence, automation, and human-centric design to improve both accuracy and investigative efficiency. By integrating advanced analytics with regulatory alignment, it empowers analysts to act faster, with greater clarity and confidence. The capabilities below outline how this next-generation approach enables that vision to materialize.

- **Contextual Detection:** Knowledge graphs reveal hidden relationships and complex transaction patterns, enabling detection of sophisticated laundering schemes.
- **Explainability:** Graph-based evidence and GenAI-powered narratives provide clear, auditable justifications for flagged transactions.
- **Scalability:** The architecture supports analysis of millions of entities and transactions in real time.
- **Natural Language Interaction:** Analysts can query the system conversationally, reducing investigation time and improving user experience.
- **Automated Compliance:** Seamless integration with FIU-IND reporting requirements ensures timely and accurate suspicious transaction reports.
- **Continuous Learning:** Human-in-the-loop feedback and ongoing data collection enhance model accuracy and adaptability.

## 1.3 Indian Regulatory Landscape

India's AML rules are based on PMLA and RBI's KYC guidelines. Reporting to FIU-IND happens through FINGate and FINnet 2.0, covering STR, CTR, CCR, CBWTR, and other formats. These systems require accurate, auditable submissions through batch or API.

# Traditional Challenges for Capturing Money Laundering

Major pain points persist today comprises of fragmented data, rules-only detection, lack of context, high false positives, and manual reporting.

- Data is fragmented across multiple platforms
- Detection relies on static rules
- Limited contextual insights
- High false-positive rates
- Manual compliance reporting

## How Graph Analytics Helps

Companies working in AML graph technology, such as Quantexa, use entity resolution and graph analysis to uncover hidden links and transaction chains. Common laundering patterns include circular transfers, structuring (smurfing), shared devices or IP addresses, sudden activity spikes, rapid layering, and round-tripping through offshore accounts.

Fraud Pattern	Graph-Based Indicator
Circular Transactions	Funds move in loops between accounts, forming closed cycles
Smurfing	Many small transactions feed into a few nodes, indicating structuring
Shared IP/Device Access	Multiple accounts connect to the same device or IP node
Dormant-to-Active Spike	A quiet node suddenly gains many edges (transactions)
Rapid Layering	Long transaction paths with short time intervals
Round-Tripping via Offshore	Funds exit and re-enter through offshore entities, often shell companies

## 2.1 Graph-Based Algorithms for AML: Circular Transactions

Detecting laundering often needs more than rules. By modeling accounts and transactions as graphs, algorithms like cycle detection can spot circular flows. Entity relationship analysis helps trace money through linked accounts or businesses.

Algorithm	Purpose	Logic and Techniques	Example Use Case
Cycle Detection Algorithm	Identify circular transactions where money flows through multiple accounts and eventually returns to the original source.	Represent accounts and transactions as a directed graph. Then, use depth-first search (DFS) to identify cycles, applying constraints such as time windows, similar amounts, and a limit on the number of hops.	change the sentence formation that resembles AI gen content.
Entity Relationship Circularity Algorithm	Finds laundering via related entities (family, companies, etc.)	Create a multi-layer graph that includes accounts, entities, and their relationships. Then, trace paths from the originator to the recipient using pattern-matching techniques and apply risk scoring along the way.	Move money through casinos, family connections, or offshore accounts.

While these algorithms are powerful, GenAI further enhances AML by enabling natural language investigations, contextual reasoning, and dynamic adaptation. The next section explains how integrating GenAI creates a more intuitive, scalable, and explainable end-to-end AML solution.

# End-to-End Conversational AML Platform: Architecture and Workflow

## User Journey:

### Analyst Investigation with Conversational AML

Consider a scenario where an AML analyst receives a real-time alert for a suspicious transaction. Using the conversational interface, the analyst queries, “*Show me all related entities and recent transactions for account X.*” The GenAI layer translates this into a graph traversal, instantly visualizing connections to shell companies and offshore accounts. The system highlights a **circular transaction pattern** and retrieves supporting documentation from compliance archives. When the analyst requests an explanation, GenAI generates a **narrative grounded in regulatory language**, ready for audit or escalation.

## Core Components of the Solution

This seamless workflow reduces investigation time from hours to minutes, enhances accuracy, and ensures regulatory traceability.

Because transaction volumes are huge, we need smart ways to process and analyze the data. This involves using algorithms that can quickly filter and highlight unusual patterns. Techniques like anomaly detection, clustering, and rule-based checks help identify transactions that don't fit the usual behavior within related networks.

## 3.1 Knowledge Graph Provides

- **Contextual Detection:** Understand the entire network of linked entities and relationships.
- **Clear Explanations:** Use graphs to show both visual and logical evidence for flagged patterns.
- **Scalable Analysis:** Handle millions of transactions and entities without performance issues.
- **Real-Time Alerts:** Spot unusual patterns as they happen.

## 3.1 Knowledge Graph Provides

- **Payment Systems:** Includes UPI, IMPS, NEFT, RTGS, AEPS, BBPS, SWIFT, digital wallets, and cryptocurrencies.
- **Sector-Specific Risks:** Covers TBML, Hawala, money mule networks, online gaming, and misuse of non-profit organizations.
- **Identity Resolution:** Uses PAN, Aadhaar, CKYC, and GSTIN for verification.

## 3.2 Challenges of LLMs

- **Risk of Hallucination:** Models can sometimes generate incorrect or made-up information.
- **Limited Enterprise Knowledge:** They don't automatically understand your internal policies or systems.
- **How to Address This:** Keep humans involved in the review process and regularly fine-tune models using enterprise-specific data.

These challenges can be overcome by having a human-in-the-loop and by collecting huge data sets and training the models.

## LangChain for Orchestrating AI Workflows

LangChain stitches together multiple analysis steps. One module handles entity links, another clusters similar behaviors, and other scores anomalies. The combined output gives the analyst a single, coherent view.

For example, if several family members share an address or show unusual patterns across different cities, the system examines those links, then applies clustering and anomaly detection to flag the case.

### Why This Matters

By merging Knowledge Graphs, GenAI reasoning, and LangChain orchestration, the platform delivers:

- **Rapid Investigations:** Hours reduced to minutes.
- **Regulatory Traceability:** Audit-ready narratives.
- **Holistic Detection:** Context-aware, multi-attribute analysis.
- **Scalable Intelligence:** Real-time monitoring across millions of transactions.

Here is the solution architecture for the conversational AML: Uncovering suspicious activity with GenAI and knowledge graphs.

### Conversational AML :

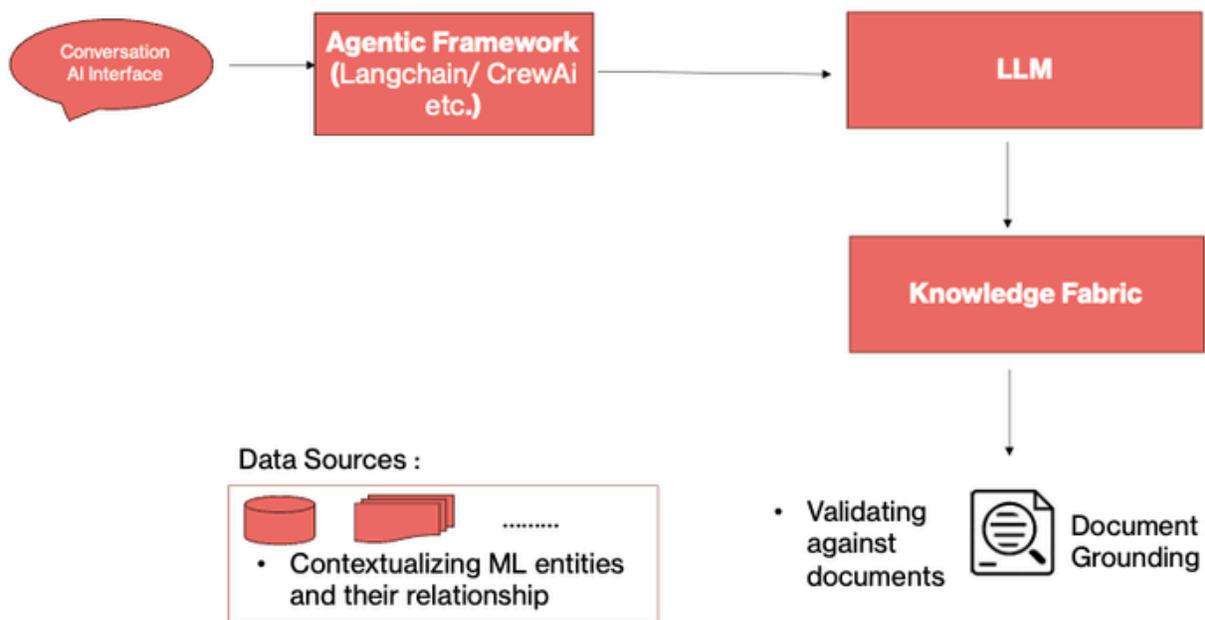


Figure 1: End-to-End Conversational AML Architecture

### 3.3 Key Components of solution

- **Knowledge Graph:** Models AML-relevant entities and relationships.
- **GenAI Layer:** Converts user queries into graph traversals and explains results.
- **Search Layer:** Grounds responses in regulatory documents.
- **UI Layer:** Chatbot or dashboard for analysts.
- **Security:** Role-based access, audit trails.

#### 3.3.1 Enterprise-Grade Architecture for Conversational AML

- **Data Ingestion and Quality:** Kafka streaming, ETL, lineage for trusted alerts.
- **Graph Design:** AML ontology + temporal modeling for evolving relationships.
- **Algorithm Portfolio:** Beyond cycles—community detection, GNNs, anomaly scoring.
- **Performance and Compliance:** Low-latency graph queries, security/privacy, audit logs.
- **Deployment Patterns:** On-prem/hybrid + DR/HA for resilience.
- **Conversational Layer Integration:** GenAI with LangChain orchestration for real-time traversal, contextual reasoning, and narrative generation.

### 3.4 Grounding Process

Grounding connects the LLM to authoritative sources to ensure answers are factually accurate, explainable, compliant, and enterprise-ready. The following steps are done during grounding:

- **Chunking:** Documents are split into manageable pieces.
- **Embedding:** Each chunk is converted into a vector using an embedding model.
- **Indexing:** These vectors are stored in a vector database (e.g., FAISS, Pinecone).
- **Retrieval:** When a query comes in, the most relevant chunks are retrieved.
- **Prompting:** These chunks are added to the LLM prompt to guide its response.

Grounding connects the LLM to authoritative sources to ensure answers are factually accurate, explainable, compliant, and enterprise-ready. The following steps are done during grounding:

- **Authoritative Sources:** FIU-IND manuals, RBI circulars, internal SOPs as primary references.
- **Citation UX:** Inline provenance for every generated insight.
- **Governance Workflows:** Approval chains and scheduled RAG refresh cadence for updated knowledge.
- **Testing Framework:** Hallucination detection, golden set validations, and stress tests for reliability.

### 3.5 Real-time Chat Interface and Uncovering Suspicious Transactions

Real-time chat interfaces are redefining AML investigations by giving analysts instant, evidence-backed answers through a single conversational query. Instead of navigating scattered systems, they can surface suspicious patterns, relationships, and documents in seconds. This turns complex financial-crime analysis into a fast, intuitive, and fully traceable workflow.

Here's an example:

A bank analyst asks the chatbot to explain why transaction x is considered suspicious.

The chatbot uses Lang chain to orchestrate the query. The LLM generates a response but ground it in:

- a) Enterprise Knowledge Graph: Links the transaction to entities like shell companies, flagged jurisdictions, or known laundering patterns.
- b) Documents: Pulls evidence from suspicious activity reports (SARs), compliance manuals, and investigation notes.

This ensures the response is not only correct but also traceable to real documents, which is essential for audit and compliance. This process can also be automated, allowing any Indian bank to report suspicious activities directly to FIU-IND, RBI, FATF or other global AML framework.

After flagging a fraudulent transaction, bank can report it to FIU-IND. Except in specific cases requiring analyst oversight, the reporting process will be automated.

### 3.6 Automated Reporting

Here are the steps for reporting to FIU-IND:

- Transaction Monitoring System → TMS Flags suspicious transaction.
- Lang Chain Orchestrator:
  - a. Queries Enterprise Knowledge Graph for entity linkages
  - b. Retrieves supporting documents from internal repositories.
  - c. Generates explanation and risk score.
- Compliance Officer Review (optional human-in-the-loop, audit trail captured)
- Submission via FINGate 2.0 (portal/batch/API), with post-submission actions tracked. (Reporting is to FIU-IND; RBI issues directions but is not the STR/CTR recipient.)

Here **FINnet Gateway (FINGate)** is the front-end portal where banks and other regulated entities register and submit mandatory reports such as Suspicious Transaction Reports (STRs), Cash Transaction Reports (CTRs), and other filings required by FIU-IND. Registration and timely reporting through FINGate are mandatory for all reporting entities under the Prevention of Money Laundering Act (PMLA).

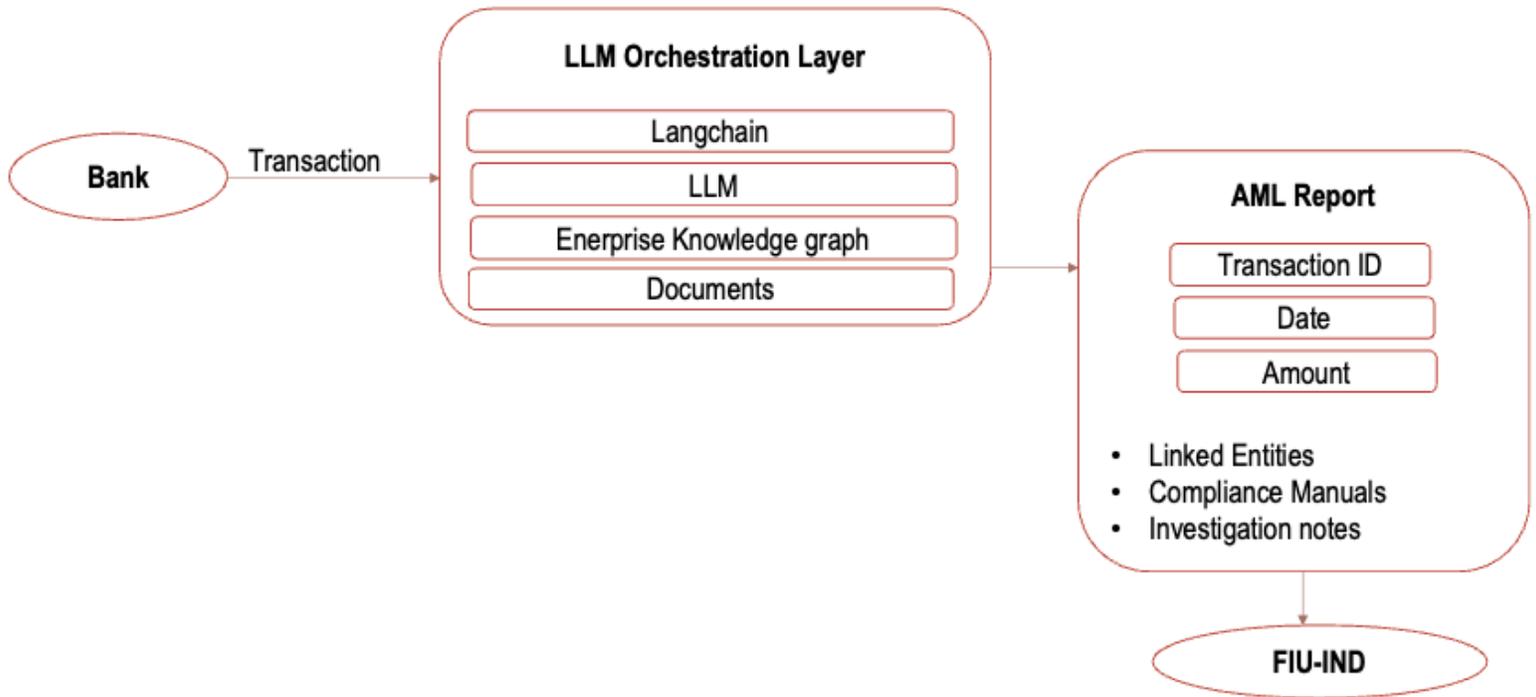


Figure 2: LLM-Enabled AML Reporting Workflow for FIU-IND

# Strategic Roadmap for Adopting GenAI-Powered AML in Indian Banking

## 5.1 Change Management and Adoption Challenges

Moving to a GenAI-powered AML platform isn't just about installing new technology. Banks also need to tackle challenges like integrating data, making old systems work together, and training analysts for new tools. Change often meets resistance, especially when AI starts influencing decisions. Success depends on strong leadership support, clear communication about the benefits, and rolling out changes in phases. Training sessions, involving stakeholders early, and keeping feedback channels open help build trust and ensure the transition delivers real value.

## 5.2 Risk, Governance, and Model Monitoring

While GenAI and knowledge graphs offer transformative potential, they introduce new risks. Model drift, data privacy breaches, and explainability gaps can undermine trust and compliance. Banks must implement robust governance frameworks, including regular model validation, bias audits, and transparent documentation. Continuous monitoring of model performance, coupled with human-in-the-loop oversight, ensures that the system adapts to evolving threats while maintaining regulatory alignment.

To successfully implement GenAI-driven AML solutions, Indian banks should follow a structured adoption path:

- Assess current AML systems to identify integration opportunities for GenAI and knowledge graphs.
- Build unified data and graph infrastructure for contextual analysis and advanced detection.
- Pilot GenAI use cases such as conversational investigations and automated reporting.
- Align with regulatory requirements by collaborating with compliance teams and FIU-IND.
- Scale and automate GenAI capabilities across business units.
- Establish continuous learning and governance with human-in-the-loop and regular audits.
- Train teams and engage stakeholders to ensure effective adoption and responsible AI use.

This approach enables banks to enhance detection, improve compliance, and future-proof their AML operations.

## 5.3 AML Lifecycle Coverage with GenAI

GenAI is reshaping the AML lifecycle by bringing context, automation, and intelligence to every step, from onboarding to ongoing monitoring and regulatory response. Instead of siloed processes, institutions can now rely on a continuously learning system that adapts to new risks and simplifies complex workflows. The areas below show how GenAI strengthens each phase of AML operations. The points below highlight how GenAI strengthens each major phase of this end-to-end AML lifecycle:

- **Customer Risk Assessment and Onboarding:** Includes CDD/EDD checks, PEP screening, UBO identification, and sanctions/adverse media reviews.
- **Continuous Monitoring Across Products:** Covers retail banking, trade finance, wallets, securities, and correspondent banking.
- **Case Management and Investigations:** Handles triage, workflows powered by natural language, and maintains audit trails.
- **Regulatory Response and Remediation:** Manages alert quality checks, STR narrative preparation, and responses to regulator queries.
- **Model and AI Operations:** Oversees version control, drift detection, bias audits, and explainability testing for models.

## About the authors



### Amit Sinha

Principal Enterprise Architect,  
LTM

Amit Sinha is a Principal Enterprise Architect at LTMindtree with over 23 years of experience. Amit has been part of the Consulting and Solution architecture COE for multiple business transformations. His domain expertise spans across BFSI, Manufacturing, Communications, Media, and Entertainment. Amit has proven experience in development, design, architecture, business process analysis and re-engineering, data modeling, system configuration, budgeting, and cloud-native solution designs. He enjoys design thinking and leading solution workshops.



### Namrata Sharma

Senior Consultant,  
LTM Research

Collaborative and vigorous with a propensity to solve problems, Namrata Sharma brings noteworthy experience within the management consulting and research domain. Namrata's areas of expertise include strategic planning, creating market intelligence studies, data modelling, and domain critical evaluation. In her tenure as Senior Consultant, Namrata analyses cutting-edge technologies, identifies strategic market opportunities, and shapes forward-looking viewpoints on transformative, beyond-the-horizon technologies as a Senior Consultant. She is currently working on analyzing potential technologies, market opportunity assessment, and creating Deep Point of Views and Beyond the horizon areas.

## Appendix

Aspect	India (PMLA, FIU-IND, RBI)	FATF (Global)	EU AMLD (Europe)	US FinCEN (USA)
Sanctions Compliance	UN sanctions, domestic lists; asset freeze	Global sanctions compliance	EU-wide and UN sanctions list	OFAC sanctions; immediate freeze and report
Data Retention	10 years minimum	Varies by jurisdiction	Typically, 5–10 years	5 years minimum
Penalties for Non-Compliance	Fines up to ₹5 lakh; license revocation; criminal liability	Country-level evaluations; reputational risk	Administrative fines; criminal sanctions	Civil and criminal penalties; enforcement actions
International Cooperation	MoUs with global bodies; FATF member	Mutual evaluations; Egmont Group	EU-wide cooperation; FIU.net	International treaties; Egmont Group
Recent Developments	RBI-FIU MoU for joint supervision; focus on fintech risks	2024 India Mutual Evaluation Report	AMLD6: criminalization, whistleblower protection	FinCEN's AML Act 2020; beneficial ownership registry

## Appendix

A table comparing Indian AML regulations (PMLA, FIU-IND, RBI) with global standards (FATF, EU AMLD, US FinCEN).

Aspect	India (PMLA, FIU-IND, RBI)	FATF (Global)	EU AMLD (Europe)	US FinCEN (USA)
Legal Framework	Prevention of Money Laundering Act (PMLA), 2002; RBI KYC Master Directions	FATF 40 Recommendations	EU AML Directives (AMLD 1–6)	Bank Secrecy Act (BSA); USA PATRIOT Act
Regulatory Bodies	FIU-IND, RBI, Enforcement Directorate	FATF (inter-governmental body)	European Commission, National FIUs	FinCEN (Financial Crimes Enforcement Network)
Scope of Coverage	Banks, NBFCs, insurance, securities, DNFBPs	All financial institutions and DNFBPs globally	All EU member states and obligated entities	Banks, MSBs, casinos, securities firms, etc
KYC/CDD Requirements	Mandatory KYC/CDD; Enhanced Due Diligence for PEPs	Risk-based CDD; EDD for high-risk clients	Strong CDD, UBO identification, EDD	CDD, EDD, Beneficial Ownership reporting
Reporting Obligations	STRs within 7 days; CTRs above ₹10 lakh; PEP reporting	STRs, CTRs, UBO disclosures	STRs, UBO registers, central databases	SARs (Suspicious Activity Reports), CTRs

## Glossary

- **FIU-IND:** Financial Intelligence Unit-India
- **RBI:** Reserve Bank of India
- **FATF:** Financial Action Task Force
- **AML:** Anti-Money Laundering
- **GenAI:** Generative AI
- **PMLA:** Prevention of Money Laundering Act, 2002
- **IP:** Intellectual Property
- **DFS:** Department of Financial Services
- **UPI:** Unified Payments Interface
- **IMPS:** Immediate Payment Service
- **NEFT:** National Electronic Funds Transfer
- **RTGS:** Real-Time Gross Settlement
- **AEPS:** Aadhar Enabled Payment System
- **BBPS:** Bharat Bill Payment System
- **SWIFT:** Society for Worldwide Interbank Financial Telecommunication
- **TBML:** Trade-Based Money Laundering
- **NPO:** Non-Profit Organization
- **PAN:** Permanent Account Number
- **CKYC:** Central Know Your Customer
- **GSTIN:** Goods and Services Tax Identification Number
- **LLMs:** Large Language Models
- **UI:** User Interface

## Glossary

- **ETL:** Extract, Transform, Load
- **GNN:** Graph Neural Network
- **DR/HA:** Disaster Recovery/High Availability
- **FAISS:** Facebook AI Similarity Search
- **SOPs:** Standard Operating Procedure
- **RAG:** Retrieval-Augmented Generation
- **UX:** User Experience
- **SARs:** Suspicious Activity Reports
- **STR:** Suspicious Transaction Report
- **JSON:** JavaScript Object Notation
- **FINGate:** Financial Intelligence Gathering Exchange
- **CDD:** Customer Due Diligence
- **EDD:** Enhanced Due Diligence
- **PEP:** Politically Exposed Person
- **UBO:** Ultimate Beneficial Owner
- **QC:** Quality Control
- **AMLD:** Anti-Money Laundering Directive
- **FinCEN:** Financial Crimes Enforcement Network
- **BSA:** Bank Secrecy Act
- **NBFBP:** Designated Non-Financial Businesses and Professions
- **NBFC:** Non-Banking Financial Company
- **KYC:** Know Your Customer
- **MoU:** Memorandum of Understanding

## References

- *FIU India Guidelines: What Every Reporting Entity Must Know*, FINLAW, May 5, 2025, [FIU India Guidelines: What Every Reporting Entity Must Know - Blog](#)
- *Reporting with FIU-IND Under PMLA*, AML India, [Reporting with FIU-IND Under PMLA](#)  
Welcome to FIU-INDIA, Financial Intelligence Unit-India, <https://fiuindia.gov.in/index.html>
- *Smurfing in AML: key alert triggers every bank should monitor*, Trapets, December 16, 2025, [Smurfing in AML: key alert triggers every bank should monitor - Trapets](#)
- *Legal Framework*, International Financial Services Centres Authority, December 24, 2025, [International Financial Services Centres Authority](#)

## About us

LTM is an AI-centric global technology services company and the Business Creativity partner to the world's largest and most disruptive enterprises. We bring human insights and intelligent systems together to help clients create greater value at the intersection of technology and domain expertise. Our capabilities span integrated operations, transformation, and business AI — enabling new ways of working, new productivity paradigms, and new roads to value. Together with over 87,000 employees across 40 countries and our global network of partners, LTM — a Larsen and Toubro company — owns business outcomes for our clients, helping them not just outperform the market, but to Outcreate it.