Comparative Analysis: India’s AML/KYC Framework vs. Global Best Practices

India’s anti-money laundering (AML) and know your customer (KYC) framework has made noteworthy progress, earning recognition from the Financial Action Task Force (FATF) by placing India in the "regular follow-up" category in 2024. This marks a strong technical compliance level, with India meeting the majority of FATF recommendations. Yet, the major challenge for India lies in closing the gap between regulation and real-world execution, particularly around real-time transaction monitoring, regular KYC updates, RegTech adoption, and oversight of Designated Non-Financial Businesses and Professions (DNFBPs).

Several recent financial crime scandals—including the Axis Bank fraud case where a fake account was opened in the name of a security force, and a large cryptocurrency Ponzi scheme exposed by the CBI—highlight these weaknesses and the urgency for improvement. Meanwhile, fraud incidents in Indian banking have surged dramatically, signaling increasing sophistication of criminals exploiting system gaps.

India’s AML/KYC Framework: Solid Foundation but Implementation Challenges

India’s AML regime is built around the Prevention of Money Laundering Act (PMLA) 2002 and supported by institutions like the Financial Intelligence Unit-India (FIU-IND), Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), and Enforcement Directorate (ED). Significant technological strides include Aadhaar-based eKYC and video KYC for faster digital onboarding, centralized customer data via the Central KYC Records Registry (CKYCR), and financial inclusion successes driven by the Jan Dhan-Aadhaar-Mobile (JAM) initiative.

Despite rapid digital adoption, operationalizing these frameworks remains challenging. Adoption of AI and machine learning in AML remains at an early stage, with only around 18% of Indian financial institutions currently deploying such technologies to automate compliance. RegTech startups are emerging, but smaller banks and regional operators lag due to limited resources, expertise, and outdated legacy systems that resist integration with advanced tools.

Global Best Practices: Learning From the Leaders

- **United States:** The US AML framework, anchored by the Bank Secrecy Act and the modern Anti-Money Laundering Act (AMLA) 2020, combines stringent legal mandates with advanced technological integration. Agencies like FinCEN ensure robust supervision. Real-time transaction monitoring is standard, powered by cutting-edge AI and machine learning solutions embedded in a mature RegTech ecosystem. The massive recent $3 billion penalty against TD Bank for failing to monitor over $18 trillion in transactions underscores the forcefulness of US enforcement.

- **Singapore:** Singapore excels in digital identity and KYC innovation, leveraging government platforms like SingPass and MyInfo for seamless, secure customer onboarding. The Monetary Authority of Singapore (MAS) fosters a strong RegTech environment through regulatory sandboxes, encouraging AI-powered fraud detection that balances innovation with compliance rigour.

- **United Kingdom:** The UK's Financial Conduct Authority (FCA) champions RegTech adoption, using AI and natural language processing to automate KYC, adverse media screening, and ongoing monitoring. Its risk-based supervisory model is agile and aligned with international standards.

- **Netherlands:** The Netherlands sets a benchmark for legal acceptance and operational deployment of AI in AML processes, thanks to a landmark court ruling validating automated AML risk monitoring. Data sharing frameworks between authorities and financial institutions streamline detection, easing compliance burdens while enhancing security.

Where India Needs to Catch Up

- **Real-Time Transaction Monitoring:** India still largely depends on post-facto analysis of transactions, delaying detection and response. In today's environment of instant payments via UPI, NEFT, and RTGS, real-time or near-real-time monitoring is critical but underdeveloped. Fragmented, non-integrated data across payment systems further hampers comprehensive oversight.

- **Periodic KYC Updates:** Despite RBI mandates requiring periodic KYC refreshes—every two years for high-risk customers and up to ten years for low-risk ones—millions of accounts face delayed updates, partly due to infrastructure limits, rural connectivity issues, and lack of user-friendly digital processes. These delays threaten both compliance and financial inclusion goals.

- **RegTech Adoption:** India's RegTech market is growing but still fragmented. Smaller banks, NBFCs, and fintech firms struggle with the cost and complexity of integrating AI-driven compliance solutions, due in part to legacy IT infrastructure and shortage of skilled personnel. Regulatory guidance on AI use in AML processes remains evolving, creating uncertainty.

- **DNFBP Supervision:** The oversight of DNFBPs—including real estate agents, lawyers, accountants, and precious metals dealers—is in its nascent stages. The FATF noted limited supervision, resulting in low levels of suspicious transaction reporting from these sectors despite their high vulnerability to money laundering. Many DNFBPs lack mandatory AML training and clear compliance protocols.

Recent Cases That Illustrate the Gaps

- **Axis Bank Fraud (2024):** An insider opened a fake account impersonating the National Security Guard, which was used for laundering illicit funds. Investigations revealed inadequate customer due diligence, poor transaction monitoring, lack of timely suspicious transaction reports (STRs), and insufficient staff training.

- **CBI Cryptocurrency Ponzi Scheme (2025):** A ₹350 crore Ponzi fraud leveraged multiple crypto exchanges, allowing seamless fund laundering across domestic and international platforms. The case exposed weak KYC and transaction monitoring especially for virtual asset service providers, underscoring the need for blockchain analytics and real-time crypto transaction oversight.

- **Banking Fraud Trends:** RBI reported a near 200% increase in the value of banking frauds in 2024-25, hitting over ₹36,000 crore. Public sector banks, relying on legacy systems and slower technology upgrades, bore the brunt. Digital payments frauds dominate in volume, while large-scale loan and advance frauds cause disproportionate losses.

What India Should Do Next

- ### Accelerate Technology Modernization and AI Integration

  Moving beyond manual and rule-based systems is vital. Indian banks and regulators should aggressively adopt AI and machine learning tools capable of spotting complex money laundering patterns in real time across multiple payment systems. Blockchain technologies can be leveraged to create immutable and transparent transaction records, enhancing cross-border cooperation and investigative efficiency.

  The RBI could promote dedicated regulatory sandboxes focused on RegTech innovation, mirroring Singapore’s model that allows fintechs to pilot new solutions under close supervision. Clear guidelines on AI governance, accountability, and explainability should accompany such innovations to maintain trust and regulatory compliance.

  Enhanced API-driven data integration between core banking, payment networks, and compliance monitoring platforms will provide a unified real-time view of customer activities, minimizing blind spots.

- ### Strengthen Regulatory Oversight and DNFBP Supervision

  India needs urgent reforms targeting partially compliant FATF areas:

Implement risk-based supervision of Non-Profit Organizations (NPOs) to prevent misuse for terrorist financing.
Clarify and enforce enhanced due diligence for domestic Politically Exposed Persons (PEPs), including source of wealth verification and ongoing monitoring.
Expand DNFBP AML oversight with mandatory training, periodic audits, and mandatory suspicious transaction reporting.
Improve coordination among DNFBP supervisors and FIU-IND to enhance data sharing and enforcement effectiveness.

- **Boost Capacity Building and Compliance Culture**

  Financial institutions must invest in continuous, scenario-based AML training that highlights emerging threats and technology usage. Building expert compliance teams with technology proficiency and investigative skills is critical.
  Formalizing academic programs and public-private partnerships can help nurture a steady stream of AML professionals attuned to India's unique compliance landscape. Training should also extend deeply into DNFBP sectors to build a culture of compliance beyond traditional banks.

- **Enhance International Cooperation and Intelligence Sharing**

  Cross-border crimes—especially in cryptocurrencies—require seamless global cooperation. India should strengthen ties with international regulatory bodies such as US FinCEN, Singapore MAS, UK FCA, and others to share threat intelligence, conduct joint investigations, and develop harmonized approaches to emerging risks involving digital assets and fintech innovations.
  Automated real-time information sharing networks, staff exchanges, and collaborative technology research can also help India stay ahead in this rapidly evolving regulatory environment.

Final Thoughts

India's AML/KYC framework is no longer theoretical—it must be effective in practice. The steady progress made over the past decade provides a strong foundation, but the path ahead demands faster technology adoption, rigorous supervisory reforms, and stronger institutional capacity. With fraud levels soaring and criminals harnessing sophisticated tools, the stakes have never been higher.
By learning from global leaders like the US, Singapore, UK, and the Netherlands, India can modernize its AML/KYC regime—not just to comply but to lead. A combination of smart regulation, cutting-edge technology, skilled human resources, and international collaboration will be the key to building a resilient and trusted financial ecosystem. Sustained commitment and action today can safeguard India's digital economy and global financial standing for decades to come.