Study Notes for
NISM-Series-XXIV: AML and CFT Provisions in Securities Markets Certification Examination

modelexam.in

NISM Exam Preparation

modelexam.in provides with basic information, study material & online model exams to help you succeed in NISM exams. (NISM – National Institute of Securities Markets – A SEBI Institute)

Both Premium (Paid)& Demo (Free) Versions are available on the website.
HARDCOPY / SOFTCOPY of the tests will NOT be provided.

Modelexam website provides ONLINE Mock Test for the following exams.

NISM Exam Mock Tests
Insurance Exams Mock Tests
JAIIB, CAIIB, IIBF Certificate Exams Mock Tests
Financial Planning Exams Mock Tests

TRAINING FOR COLLEGE STUDENTS

Training can be given for MBA, M.Com, B.Com & BBA students to pass NISM exams. This will help them to get placed in Banks, Share broking Offices, Mutual Fund Companies etc.

Kindly Whatsapp **98949 49987** for queries on training for NISM Certifications.

Examination Details

Total Questions	**50 X 1 Marks**
Total marks	**50**
Type	**Multiple Choice**
Pass Score	**50% = 25 marks**
Duration	**1 Hour**
Negative marks	**-**

Chapterwise - Weightage

Sr. No.	Chapter Name	Weightage
Part A		
1	Introduction to Anti Money Laundering (AML), Combating the Financing of Terrorism (CFT) and Proliferation Financing (PF)	6
2	Prevention of Money Laundering Act, 2002 (PMLA)	8
3	The Prevention of Money-laundering (Maintenance of Records) Rules, 2005	8
Part B		
4	Scheduled Offences	3
5	Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT) and Proliferation Financing (PF) Guidelines	5
6	SEBI Guidelines for Anti Money Laundering (AML) Standards, Combating the Financing of Terrorism (CFT) and Proliferation Financing (PF)	7
7	SEBI guidelines for KYC norms in Securities Market	8
8	Discussion on PMLA related Cases	5
Total Marks		**50**

NISM-Series-XXIV: AML and CFT Provisions in Securities Markets Certification Examination

Chapter-1 Introduction to Anti Money Laundering (AML), Combating the Financing of Terrorism (CFT) and Proliferation Financing (PF)

Money Laundering Definition: Money laundering involves disguising the source, changing the form, or moving profits of criminal acts to make them appear legitimate.

Purpose of AML Laws: AML laws prevent criminals from hiding illegally obtained money, safeguarding the financial system's integrity.

CFT Objective: Combating the Financing of Terrorism (CFT) aims to disrupt funding for terrorist activities to ensure global financial stability.

Proliferation Financing (PF): PF refers to financing the spread of weapons of mass destruction, addressed alongside AML and CFT.

Money Laundering Process: Money laundering occurs in three stages: placement, layering, and integration.

Placement Stage: Placement involves introducing illicit funds into the financial system, often through cash deposits or smurfing.

Layering Stage: Layering conceals the source of funds through complex transactions, making it difficult to trace.

Integration Stage: Integration reintroduces laundered funds into the legitimate financial system for use without suspicion.

Global AML Initiatives: The Financial Action Task Force (FATF) sets global standards to combat money laundering and terrorist financing.

FATF Membership: India became a FATF member in 2010, also participating in Asia Pacific Group (APG) and Eurasian Group (EAG).

Bank Secrecy Act (BSA): The U.S. enacted the BSA in 1970, requiring financial institutions to report cash transactions over $10,000.

FATF Standards Update: FATF revised its standards in 2023 to address evolving money laundering techniques.

Indian AML Framework: India's Prevention of Money Laundering Act (PMLA), 2002, combats the legalization of illegal proceeds.

FIU-IND Role: Financial Intelligence Unit-India (FIU-IND) receives, analyzes, and disseminates financial transaction reports.

Smurfing Technique: Smurfing involves breaking large illicit sums into smaller deposits below reporting thresholds.

Mule Accounts: Mule accounts are controlled by someone other than the account holder, often used for laundering.

BIS Role: The Bank for International Settlements (BIS) supports AML by facilitating central bank cooperation and issuing guidelines.

PMLA Enactment: The PMLA, 2002, enables confiscation of property derived from illegal activities.

Scheduled Offences: PMLA covers scheduled offences under various acts, including SEBI and Companies Act.

Global Cooperation: AML/CFT efforts require international collaboration to address cross-border financial crimes.

Terrorist Financing: Terrorist financing involves funds from both legal and illegal sources to support terrorist activities.

FATF Grey List: Jurisdictions under increased monitoring by FATF are on the grey list for strategic deficiencies.

AML Policy Importance: Financial institutions implement AML policies to detect and prevent illicit activities.

Criminal Proceeds: Proceeds of crime are properties obtained from scheduled offences under PMLA.

FIU-IND Establishment: FIU-IND was established in 2004 as India's central agency for AML/CFT.

PMLA Guidelines: PMLA mandates reporting entities to detect and report suspicious transactions.

Layering Challenges: Layering creates complex transaction trails to obscure the origin of illicit funds.

Integration Methods: Laundered funds are integrated via investments in legitimate businesses or assets.

BSA Requirements: BSA mandates record-keeping of cash purchases and suspicious activity reporting.

India's FATF Role: India's FATF membership enhances its global AML/CFT compliance efforts.

BIS Guidelines: BIS issues guidelines on managing risks related to money laundering.

PMLA Scope: PMLA applies to financial institutions, intermediaries, and designated businesses.

AML Evolution: AML laws evolved post-9/11 to include combating terrorist financing.

Smurfing Risks: Smurfing avoids detection by keeping transactions below AML reporting limits.

Mule Account Control: Mule accounts are often controlled by third parties for illicit transactions.

FIU-IND Reporting: FIU-IND coordinates with national and international agencies for AML/CFT enforcement.

Global AML Standards: FATF's 40 Recommendations guide global AML/CFT frameworks.

Indian AML History: India's AML laws were strengthened post-2002 with PMLA enactment.

Cross-Border Implications: PMLA addresses offences with cross-border implications in its schedule.

Placement Risks: Placement is risky for criminals due to potential suspicion during fund entry.

Layering Techniques: Layering may involve wire transfers or offshore accounts to hide funds.

Integration Goals: Integration aims to make illicit funds appear legitimate for use.

FATF Regional Bodies: APG and EAG support FATF's regional AML/CFT efforts.

BIS Research: BIS conducts research to enhance monetary and financial stability.

FIU-IND Independence: FIU-IND reports directly to the Economic Intelligence Council.

PMLA Penalties: PMLA imposes penalties for non-compliance with reporting obligations.

AML Compliance: Financial institutions must evolve internal mechanisms for AML compliance.

Terrorist Financing Sources: Funds for terrorism may come from legal sources like donations.

FATF Monitoring: FATF monitors jurisdictions for compliance with AML/CFT standards.

PMLA Reporting: Reporting entities must furnish transaction information to FIU-IND.

AML Technology: Technology-driven solutions enhance AML/CFT compliance efforts.

Chapter-2 Prevention of Money Laundering Act, 2002

PMLA Objective: PMLA, 2002, aims to prevent, detect, and prosecute money laundering activities.

Money Laundering Offence: Section 3 defines money laundering as engaging with proceeds of crime.

Section 4 Penalty: Section 4 prescribes 3-7 years imprisonment and fines for money laundering.

Reporting Entities: Reporting entities include banks, financial institutions, and intermediaries.

Record Maintenance: Section 12 mandates maintaining transaction records for five years.

Suspicious Transactions: Reporting entities must report suspicious transactions to FIU-IND.

Principal Officer: Each reporting entity must appoint a Principal Officer for PMLA compliance.

Directorate of Enforcement: The Directorate enforces PMLA and investigates money laundering.

FIU-IND Functions: FIU-IND analyzes and disseminates financial intelligence to authorities.

Scheduled Offences: PMLA covers offences listed in its schedule, including SEBI Act violations.

Client Due Diligence: Reporting entities must verify client identity and beneficial owners.

Record Confidentiality: Transaction records must be kept confidential unless required by law.

Cash Transaction Reporting: Transactions over ₹10 lakh must be reported to FIU-IND.

Cross-Border Transfers: Wire transfers above ₹5 lakh require reporting.

PMLA Definitions: PMLA defines terms like “proceeds of crime” and “attachment.”

Beneficial Owner: The beneficial owner is the natural person controlling a client or entity.

Appellate Tribunal: The Appellate Tribunal handles appeals under PMLA.

Special Court: Special Courts are designated for PMLA offence trials.

Transaction Records: Records of client identity must be maintained for five years post-relationship.

PMLA Scope: PMLA applies to individuals, companies, trusts, and other entities.

Proceeds of Crime: Property derived from scheduled offences is considered proceeds of crime.

Suspicious Transaction Definition: Suspicious transactions lack economic rationale or involve terrorism financing.

PMLA Enforcement: The Directorate of Enforcement investigates PMLA violations.

Client Identity Records: Entities must maintain client identity documents for compliance.

Cross-Border Offences: PMLA addresses offences with international implications.

PMLA Rules: PML Rules specify transaction reporting and record maintenance procedures.

Principal Officer Role: The Principal Officer ensures compliance with PMLA reporting.

FIU-IND Coordination: FIU-IND coordinates with enforcement agencies globally.

Record Retention: Transaction records must be preserved for five years.

Suspicious Transaction Criteria: Transactions with unusual complexity or no bona fide purpose are suspicious.

PMLA Penalties: Non-compliance with PMLA can lead to fines and imprisonment.

Client Verification: Entities must verify client identity at account opening.

Directorate Functions: The Directorate enforces PMLA, FEMA, and FEOA.

FIU-IND Reporting: FIU-IND receives cash and suspicious transaction reports.

PMLA Coverage: PMLA covers banking companies, NBFCs, and intermediaries.

Beneficial Owner Identification: Entities must identify beneficial owners of clients.

Record Maintenance Period: Client records are retained for five years after transactions.

Suspicious Transaction Reporting: STRs must be filed promptly with FIU-IND.

PMLA Amendments: PMLA has been updated to align with global AML standards.

Client Due Diligence Process: CDD involves verifying client identity and transaction purpose.

FIU-IND Establishment: FIU-IND was set up in 2004 under the Ministry of Finance.

PMLA Confidentiality: Information furnished under PMLA must remain confidential.

Cross-Border Reporting: Cross-border wire transfers above ₹5 lakh are reportable.

Principal Officer Appointment: Reporting entities must appoint a senior officer as Principal Officer.

Suspicious Transaction Monitoring: Entities must monitor transactions for suspicious activity.

PMLA Legal Framework: PMLA provides a legal framework for confiscating illicit proceeds.

Directorate Mandate: The Directorate investigates money laundering and foreign exchange violations.

FIU-IND Independence: FIU-IND operates independently under the Finance Ministry.

PMLA Compliance: Reporting entities must comply with PMLA and PML Rules.

Transaction Reporting: Cash transactions above ₹10 lakh require mandatory reporting.

Client Record Updates: Entities must periodically update client records for compliance.

Chapter-3 The Prevention of Money-laundering (Maintenance of Records) Rules, 2005

PML Rules Objective: PML Rules, 2005, provide guidelines for implementing PMLA provisions.

Record Maintenance: Rule 3 mandates maintaining records of specified transactions.

Cash Transactions: All cash transactions above ₹10 lakh must be recorded.

Cross-Border Transfers: Wire transfers over ₹5 lakh require reporting.

Client Due Diligence: Rule 9 mandates verifying client identity and beneficial owners.

Central KYC Registry: KYC records must be filed with the Central KYC Registry within 10 days.

Suspicious Transactions: Rule 3 requires reporting transactions suspected of involving proceeds of crime.

Principal Officer Role: Rule 7 mandates reporting entities to appoint a Principal Officer.

Record Retention: Transaction records must be retained for 10 years.

Group-Wide Policies: Rule 3A requires group-wide AML/CFT policies for information sharing.

KYC Verification: Entities must verify client identity at account opening.

Suspicious Transaction Reporting: STRs must be filed with FIU-IND promptly.

Digital KYC: KYC can be conducted digitally using Aadhaar or other valid documents.

Beneficial Owner: Rule 9 defines beneficial owners as those with controlling ownership.

Central KYC Functions: The Central KYC Registry stores and retrieves KYC records.

Aadhaar Authentication: Aadhaar-based e-KYC is a valid KYC verification method.

Record Confidentiality: KYC records must remain confidential unless authorized.

Client Due Diligence Process: CDD involves identifying clients and verifying their purpose.

Transaction Monitoring: Entities must monitor transactions for suspicious activity.

KYC Record Upload: KYC records must be uploaded to the Central KYC Registry.

Non-Profit Organizations: Non-profits must register on the DARPAN Portal for KYC.

Small Accounts: Small accounts have relaxed KYC requirements for limited transactions.

Aadhaar Voluntary Use: Aadhaar submission for KYC is optional and voluntary.

Digital Signature: KYC documents can be authenticated using electronic signatures.

High-Risk Clients: Enhanced due diligence is required for high-risk clients.

Record Retrieval: Records must be easily retrievable for competent authorities.

Suspicious Transaction Criteria: Transactions with no economic rationale are suspicious.

KYC Updates: Client KYC records must be updated periodically.

Third-Party KYC: KYC records from third parties must meet PMLA requirements.

Client Identity Verification: Entities must verify client identity using reliable sources.

Cross-Border Wire Transfers: Transfers above ₹5 lakh are reportable.

Group Information Sharing: Groups must share information for AML/CFT compliance.

KYC Accessibility: Central KYC records must be accessible in real-time.

Suspicious Transaction Monitoring: Entities must have systems to detect suspicious activity.

Aadhaar QR Code: QR codes on Aadhaar can auto-populate KYC details.

Digital KYC Process: Digital KYC involves OTP-based client verification.

Record Maintenance Period: KYC records are retained for 10 years post-relationship.

Non-Profit KYC: Non-profits require additional KYC registration on DARPAN.

Client Due Diligence Timing: CDD is conducted at account opening and periodically.

Suspicious Transaction Reports: STRs include attempted transactions.

KYC Record Storage: The Central KYC Registry safeguards KYC records.

Aadhaar Exemptions: Exemptions exist for clients unable to provide Aadhaar.

Digital KYC Accessibility: Guidelines ensure digital KYC inclusivity for disabled persons.

Transaction Reporting: Cash transactions below ₹10 lakh but connected are reportable.

Principal Officer Reporting: The Principal Officer files transaction reports to FIU-IND.

KYC for Foreign Nationals: Foreign nationals require overseas address proof.

Client Record Updates: Entities must update client records based on risk.

Suspicious Transaction Definition: Suspicious transactions may involve terrorism financing.

KYC Record Confidentiality: KYC records cannot be shared without authorization.

Digital KYC OTP: OTP verification serves as a client signature for KYC.

Group-Wide AML Programs: Groups must implement AML/CFT programs across entities.

Chapter-4 Scheduled Offences

Scheduled Offences: Scheduled offences under PMLA are listed in Parts A, B, and C.

Part A Offences: Part A includes serious crimes with no monetary threshold, e.g., under the Indian Penal & Narcotics Acts.

Part B Offences: Part B includes tax-related offences with a ₹3 million or ₹10 million threshold.

Part C Offences: Part C covers cross-border offences from Parts A and B.

SEBI Act Offences: Violations under the SEBI Act are scheduled offences under PMLA.

Companies Act Offence: Section 447 (fraud) of the Companies Act, 2013, is a scheduled offence.

Indian Penal Code: Offences like extortion, robbery, and counterfeiting are scheduled under Part A.

Narcotics Act: Contraventions related to drugs are scheduled offences.

Unlawful Activities Act: Offences under the UAP Act, 1967, are included in Part A.

Arms Act: Arms-related offences under the Arms Act, 1959, are scheduled.

Prevention of Corruption: Corruption offences under the 1988 Act are scheduled.

Wildlife Protection Act: Offences under the Wildlife Protection Act are included.

Copyright Act: Copyright violations are scheduled offences under PMLA.

Trademark Act: Trademark infringements are part of scheduled offences.

Information Technology Act: IT Act violations are included in the PMLA schedule.

Customs Act: False declarations under the Customs Act, 1962, are Part B offences.

Cross-Border Implications: Part C addresses offences with international implications.

Bharatiya Nyaya Sanhita: BNS 2023 offences are covered under Part A.

Antiquities Act: Violations of the Antiquities and Art Treasures Act are scheduled.

Immoral Traffic Act: Prostitution-related offences are scheduled under PMLA.

Explosive Substances Act: Offences involving explosives are included in Part A.

Maritime Navigation Act: Offences against maritime safety are scheduled offences.

Plant Varieties Act: False denomination under the 2001 Act is a scheduled offence.

Proceeds of Crime: Scheduled offences generate proceeds of crime under PMLA.

Monetary Threshold: Part B offences require a minimum value for applicability.

Cross-Border Offences: Part C includes offences against property under IPC.

Black Money Act: Tax evasion under the 2015 Black Money Act is a scheduled offence.

Extortion Offences: IPC sections 384-389 cover extortion as scheduled offences.

Robbery and Dacoity: IPC sections 392-402 are scheduled offences.

Counterfeiting Currency: IPC section 489A covers counterfeiting as a scheduled offence.

Kidnapping for Ransom: IPC section 364A is a scheduled offence under PMLA.

Attempt to Murder: IPC section 307 is a scheduled offence.

Drug Contraventions: NDPS Act sections 15, 18, and 27A are scheduled offences.

Unlawful Association: UAP Act section 10 is a scheduled offence.

Arms Contravention: Arms Act section 26 violations are scheduled offences.

Prostitution Offences: Immoral Traffic Act sections 5-9 are scheduled.

Environmental Offences: Wildlife Protection Act violations are scheduled.

Tax Evasion: Black Money Act section 51 offences are scheduled.

Fraud under Companies Act: Section 447 fraud is a key scheduled offence.

Customs Violations: Customs Act section 132 offences are Part B scheduled offences.

Cross-Border Property Offences: IPC Chapter XVII offences are included in Part C.

Narcotics Violations: NDPS Act violations are critical scheduled offences.

Corruption Offences: Prevention of Corruption Act offences are scheduled.

Maritime Safety Offences: Maritime Navigation Act section 3 is scheduled.

Plant Variety Offences: False denomination under the 2001 Act is scheduled.

IT Act Violations: Information Technology Act offences are scheduled.

Antiquities Violations: Antiquities Act offences are included in the schedule.

Proceeds of Crime Link: Money laundering requires proceeds from scheduled offences.

Part A Seriousness: Part A offences are serious with no monetary threshold.

Part B Threshold: Part B offences require a ₹3 million or ₹10 million threshold.

Part C Scope: Part C focuses on cross-border implications of scheduled offences.

Chapter-5 Anti Money Laundering (AML), Combating the Financing of Terrorism (CFT) and Proliferation Financing (PF) Guidelines

AML/CFT Guidelines: Guidelines aim to prevent money laundering and terrorist financing.

CFT Scope: CFT guidelines address funding for terrorist activities under UAP Act.

PF Guidelines: PF guidelines prevent financing of weapons of mass destruction.

Financial Service Providers: SPs must comply with AML/CFT/PF obligations.

Virtual Digital Assets: VDAs convertible to fiat are subject to AML/CFT guidelines.

UAP Act Powers: Section 5.1A allows freezing of terrorist-related funds.

Guideline Applicability: Guidelines apply to all registered intermediaries and VDAs.

Risk-Based Approach: SPs must adopt a risk-based approach to AML/CFT.

Suspicious Transaction Reporting: SPs must report suspicious transactions to FIU-IND.

Client Due Diligence: CDD is mandatory for identifying clients and beneficial owners.

FATF Grey List: Jurisdictions under increased monitoring are on the FATF grey list.

VDA Compliance: VDA providers must implement AML/CFT/PF measures.

Terrorist Financing: Funds for terrorism may come from legal or illegal sources.

PMLA Compliance: Guidelines align with PMLA and PML Rules requirements.

FIU-IND Role: FIU-IND coordinates AML/CFT efforts nationally and globally.

Risk Management: SPs must manage ML/TF risks through robust policies.

Client Verification: Verifying client identity is critical for AML compliance.

Reporting Mechanism: Efficient reporting prevents ML, TF, and PF activities.

VDA Guidelines: Guidelines focus on VDAs intersecting with the fiat system.

Central Bank Digital Currencies: CBDCs are excluded from VDA AML guidelines.

Global AML Standards: FATF standards guide AML/CFT/PF compliance.

UAP Act Enforcement: UAP Act prohibits transactions supporting terrorism.

SP Obligations: SPs must implement group-wide AML/CFT programs.

Suspicious Transaction Criteria: Transactions lacking economic rationale are suspicious.

FIU-IND Reporting: SPs report suspicious transactions to FIU-IND.

Risk Assessment: SPs assess ML/TF risks for new products and services.

Guideline Updates: Guidelines are updated to reflect evolving financial crimes.

VDA Risk Management: VDA providers must mitigate ML/TF risks.

Terrorist Asset Freezing: UAP Act allows freezing of terrorist-related assets.

AML Policy Implementation: SPs must implement AML policies promptly.

Client Record Maintenance: Records of client transactions must be maintained.

Suspicious Transaction Monitoring: SPs must monitor transactions for suspicious activity.

Global Cooperation: AML/CFT requires international collaboration.

VDA Convertible Funds: Guidelines apply to VDAs convertible to other funds.

FIU-IND Coordination: FIU-IND coordinates with enforcement agencies.

Risk-Based Monitoring: Monitoring must be sensitive to ML/TF risks.

PMLA Alignment: Guidelines align with PMLA's reporting requirements.

VDA Service Providers: VDA SPs have specific AML/CFT obligations.

Terrorist Financing Prevention: Guidelines aim to disrupt terrorist funding.

Client Due Diligence Timing: CDD is conducted at account opening and periodically.

FATF Monitoring: FATF monitors jurisdictions for AML/CFT compliance.

VDA Risk Assessment: VDA providers assess risks for new products.

UAP Act Provisions: UAP Act prohibits transactions with terrorist entities.

Guideline Scope: Guidelines cover all financial institutions and intermediaries.

Suspicious Transaction Definition: Suspicious transactions may involve terrorism financing.

VDA Compliance Challenges: VDA providers face unique AML/CFT challenges.

FIU-IND Independence: FIU-IND operates independently under the Finance Ministry.

Risk-Based Policies: SPs must adopt risk-based AML/CFT policies.

Client Identity Verification: Verifying client identity is mandatory for SPs.

AML/CFT Training: SPs must train staff on AML/CFT compliance.

Guideline Effectiveness: Guidelines ensure effective AML/CFT implementation.

Chapter-6 SEBI Guidelines for Anti Money Laundering (AML) Standards, Combating the Financing of Terrorism (CFT) and Proliferation Financing (PF)

SEBI Guidelines: SEBI guidelines ensure AML/CFT/PF compliance for intermediaries.

Master Circular: SEBI's Master Circular dated June 06, 2024, outlines AML/CFT norms.

Risk-Based Approach: Intermediaries must adopt a risk-based approach to ML/TF risks.

Client Due Diligence: CDD involves verifying client identity and beneficial owners.

Suspicious Transaction Reporting: Intermediaries must report STRs to FIU-IND.

AML Policy: Intermediaries must maintain written AML procedures.

Client Acceptance Policy: Policies must identify high-risk clients for ML/TF.

Beneficial Owner: Beneficial owners hold over 10% of company shares or profits.

Politically Exposed Persons: PEPs require enhanced due diligence.

High-Risk Clients: NRIs, HNIs, and trusts are considered high-risk clients.

Transaction Monitoring: Intermediaries must monitor transactions for suspicious activity.

Record Retention: Records must be retained for 10 years under PML Rules.

Suspicious Transaction Definition: Suspicious transactions lack economic rationale.

Client Identification Procedure: CIP is conducted at account opening and transactions.

Risk Management: Intermediaries must manage ML/TF risks proactively.

FIU-IND Reporting: STRs are reported to FIU-IND's Director.

Third-Party Reliance: Intermediaries may rely on third-party CDD if regulated.

High-Risk Countries: Clients from high-risk countries require enhanced scrutiny.

Staff Training: Intermediaries must train staff on AML/CFT vigilance.

Policy Review: AML policies must be reviewed regularly for effectiveness.

Client Record Updates: Client records must be updated periodically.

Suspicious Transaction Monitoring: Systems must detect and report suspicious activity.

Non-Profit Organizations: Non-profits require DARPAN Portal registration.

Enhanced Due Diligence: Enhanced CDD is required for high-risk clients.

Transaction Records: Records must be available to investigating authorities.

Client Risk Classification: Clients are classified based on ML/TF risk levels.

SEBI Circular Compliance: Intermediaries must comply with SEBI AML circulars.

PEP Identification: Systems must identify clients as politically exposed persons.

Record Confidentiality: Transaction records must remain confidential.

Risk Assessment: New products and services require ML/TF risk assessments.

Client Due Diligence Timing: CDD is conducted at account opening and periodically.

Suspicious Transaction Reports: STRs include attempted transactions.

High-Risk Client Monitoring: High-risk clients require enhanced transaction scrutiny.

AML Policy Implementation: AML policies must be implemented promptly.

FIU-IND Contact: FIU-IND's contact details are provided for reporting.

Client Record Retention: Records are retained for periods exceeding SEBI requirements.

Third-Party KYC: Third-party KYC must meet PMLA standards.

Suspicious Transaction Criteria: Transactions with unusual complexity are suspicious.

Risk-Based Monitoring: Monitoring must be sensitive to ML/TF risks.

Client Identification: CIP ensures intermediaries know their clients.

SEBI Oversight: SEBI monitors compliance through audits and inspections.

Record Retrieval: Records must be easily retrievable for authorities.

Non-Profit KYC: Non-profits require additional KYC documentation.

Transaction Reporting: STRs are reported to higher authorities within intermediaries.

High-Risk Client Categories: CSCs include PEPs, NRIs, and NGOs.

AML Policy Updates: Policies must be updated to reflect new risks.

Client Due Diligence Process: CDD includes verifying client purpose and identity.

Suspicious Transaction Analysis: Intermediaries analyze transactions for suspicious nature.

SEBI Circular Dates: Key circulars include June 06, 2024, and December 19, 2022.

Record Maintenance: Intermediaries must maintain records per PML Rules.

Client Risk Management: Risk-based approaches mitigate ML/TF risks.

Chapter-7 SEBI Guidelines for KYC Norms in Securities Market

KYC Guidelines: SEBI mandates KYC for all intermediaries at account opening.

Proof of Identity: PoI includes Aadhaar, passport, or voter ID.

Proof of Address: PoA includes utility bills or Aadhaar.

Permanent Account Number: PAN is mandatory for securities market participants.

Central KYC Registry: KYC records are uploaded to CKYCR within 3 days.

Digital KYC: Digital KYC uses Aadhaar or electronic signatures.

Non-Individual KYC: Legal entities require additional documents like registration certificates.

Aadhaar Voluntary: Aadhaar use for KYC is optional and voluntary.

Client Due Diligence: CDD verifies client identity and business purpose.

KYC Record Updates: Client records must be updated periodically.

Suspicious Transaction Reporting: Intermediaries report STRs to FIU-IND.

Mobile and Email: Client mobile and email details are uploaded to KRA.

Video IPV: Video In-Person Verification is allowed for KYC.

Aadhaar Authentication: Aadhaar e-KYC is a valid KYC method.

Non-Profit KYC: Non-profits register on the DARPAN Portal.

High-Risk Clients: Enhanced due diligence is required for CSCs.

KYC Record Retention: KYC records are retained for 10 years.

Third-Party Address: Third-party addresses can be used with client consent.

Foreign Nationals: Foreign nationals require overseas address proof.

KYC Form Parts: KYC form includes Part I (general) and Part II (specific).

e-PAN Acceptance: e-PAN is a valid PoI for KYC compliance.

SARAL Account: Simplified KYC for resident individuals via SARAL form.

KRA Upload: Intermediaries upload KYC to KRA within 3 days.

Client Record Confidentiality: KYC records must remain confidential.

Digital KYC Accessibility: Guidelines ensure inclusivity for disabled persons.

Aadhaar QR Code: QR codes auto-populate KYC details.

KYC Verification: Intermediaries verify client identity using reliable sources.

Non-Individual Documents: Legal entities submit registration and financial documents.

PEP Identification: Intermediaries identify politically exposed persons.

KYC Record Storage: CKYCR stores and retrieves KYC records.

Digital Signature: KYC documents can be signed electronically.

Client Due Diligence Timing: CDD is conducted at account opening.

High-Risk Client Monitoring: CSCs require enhanced scrutiny.

KRA Compliance: Stock exchanges monitor KYC compliance via audits.

Aadhaar Exemptions: Exemptions exist for clients unable to provide Aadhaar.

KYC for Trusts: Trusts submit trust deeds and trustee details.

SARAL Form: SARAL form simplifies KYC for resident individuals.

Foreign Address Proof: Foreign nationals submit embassy-issued address proof.

KYC Record Updates: Intermediaries update KYC data periodically.

Client Risk Assessment: KYC processes assess client ML/TF risks.

Aadhaar e-KYC: e-KYC uses Aadhaar authentication services.

Non-Profit Registration: Non-profits require DARPAN Portal registration.

KYC Record Retrieval: Records must be easily retrievable for authorities.

Client Identification: KYC ensures intermediaries know their clients.

Digital KYC OTP: OTP verification serves as a client signature.

KYC for HUFs: HUFs submit deeds and bank statements.

Suspicious Transaction Monitoring: KYC aids in detecting suspicious activity.

KRA Data Upload: Intermediaries ensure no KYC data duplication in KRA.

SEBI Oversight: SEBI ensures KYC compliance through inspections.

Client Record Maintenance: Electronic KYC records reduce physical storage needs.

Chapter-8 Discussion on PMLA related Cases

Way2Wealth Case: Way2Wealth failed to file STRs, incurring a ₹1 lakh penalty.

SKSE Securities: SKSE delayed AML policy implementation, fined ₹2 lakh.

Raima Equities: Raima lacked a PEP identification system, fined ₹2 lakh.

Marfatia Case: Marfatia's procedural lapses did not warrant a penalty.

Shreepati Holdings: Shreepati delayed AML compliance, fined ₹40 lakh.

BOISL Case: BOISL's delayed AML policy led to a ₹40 lakh penalty.

Paytm Payments Bank: Paytm violated PMLA obligations, fined ₹5.49 crore.

Bybit Fintech: Bybit violated PMLA rules, fined ₹9.27 crore.

STR Reporting: Failure to report suspicious transactions leads to penalties.

AML Policy Delays: Delays in AML policy implementation attract fines.

PEP Identification: Lack of PEP identification systems violates SEBI guidelines.

Suspicious Transaction Monitoring: Inadequate STR monitoring leads to penalties.

FIU-IND Enforcement: FIU-IND imposes penalties under Section 13 of PMLA.

SEBI Inspections: SEBI conducts inspections to ensure AML compliance.

Principal Officer Role: Principal Officers must handle STRs effectively.

PMLA Violations: Violations of PMLA result in monetary penalties.

Case Findings: Cases highlight deficiencies in AML/CFT mechanisms.

SEBI Circular Compliance: Intermediaries must comply with SEBI AML circulars.

Penalty Proportionality: Penalties are proportional to the violation's severity.

Suspicious Transaction Alerts: Ignoring alerts from exchanges violates regulations.

AML Policy Implementation: Timely AML policy adoption is mandatory.

Inspection Findings: SEBI inspections identify AML compliance gaps.

STR Closure: Closing STRs without reasons violates PMLA.

Delayed Compliance: Delayed rectification of deficiencies incurs penalties.

SEBI Penalty Powers: Section 15HB of SEBI Act allows monetary penalties.

FIU-IND Orders: FIU-IND issues orders under Section 13 for violations.

Case Precedents: Penalties set precedents for AML compliance.

Paytm Violations: Paytm failed to discharge Chapter IV PMLA obligations.

Bybit Violations: Bybit violated multiple PMLA rules, leading to a high penalty.

AML Policy Framework: SEBI requires a robust AML policy framework.

Suspicious Transaction Handling: Proper STR handling is critical for compliance.

SEBI Circular Dates: Key circulars include January 18, 2006, and March 12, 2014.

Penalty Appeals: Securities Appellate Tribunal may reduce excessive penalties.

AML Inspection: Inspections ensure intermediaries comply with AML norms.

STR Reporting Delays: Delays in STR filing violate PMLA rules.

Client Due Diligence: Inadequate CDD leads to regulatory penalties.

PMLA Section 13: Section 13 empowers FIU-IND to impose fines.

SEBI Adjudication: SEBI adjudicates AML violations under Section 15HB.

Compliance Rectification: Deficiencies must be rectified promptly post-inspection.

Suspicious Transaction Analysis: Intermediaries must analyze STRs thoroughly.

PEP Systems: Lack of PEP identification systems incurs penalties.

AML Policy Updates: Policies must be updated to reflect SEBI guidelines.

Case Outcomes: Cases emphasize timely AML/CFT compliance.

FIU-IND Penalties: FIU-IND imposes significant fines for PMLA violations.

SEBI Oversight: SEBI monitors intermediaries for AML compliance.

STR Monitoring Systems: Robust STR monitoring systems are mandatory.

Penalty Factors: Penalties consider violation severity and compliance history.

AML Policy Adoption: Intermediaries must adopt AML policies within 30 days.

Suspicious Transaction Reports: STRs include attempted transactions.

Regulatory Compliance: Intermediaries must comply with PMLA and SEBI rules.

Case Studies Importance: Case studies illustrate practical PMLA implementation.

==========

IMPORTANT NOTE :

1. Attend **ALL** Questions.
2. For the questions you don't know the right answer – Try to eliminate the wrong answers and take a guess on the remaining answers.
3. DO NOT MEMORISE the questions & answers. It's not the right to way to prepare for any NISM exam. Good understanding of Concepts is essential.

July 2025

All the Best ☺

MODELEXAM

Online Mock tests for NISM, IIBF, IRDA & FP Exams

94, 1st Floor, TPK Road, Andalpuram, Madurai – 625 003.

Email: akshayatraining@gmail.com

WhatsApp only - 98949 49987