Study Notes for NISM IFSCA 01 : Certification Course on Anti Money Laundering and Counter Terrorist Financing in the IFSC

NISM IFSCA 01 : Examination Details

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

Chapterwise Weightage

Sr. No.	Chapter Name	Weightages
Part A – General Rules and Regulations related to Anti-Money Laundering in India		
1	Introduction to Anti Money Laundering (AML), Combating the Financing of Terrorism (CFT) and Proliferation Financing (PF)	5
2	Prevention of Money Laundering Act, 2002	7
3	The Prevention of Money-laundering (Maintenance of Records) Rules, 2005	7
4	Scheduled Offences	3
Part B – IFSCA Regulations for Anti Money Laundering (AML), Counter-Terrorist Financing (CTF) and Know Your Customer (KYC)		
5	IFSCA (Anti Money Laundering, Counter Terrorist-Financing and Know Your Customer) Guidelines, 2022	8
6	IFSCA Guidelines for KYC norms	10
7	Discussion on PMLA related Cases	4
8	Financial Action Task Force and Its Recommendations on AML and CFT	6
Total Marks		**50**

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

Money Laundering : Money laundering is the process of disguising criminal proceeds to hide their illegal origin.

Criminal Proceeds : Illegal arms sales, smuggling, organised crime, drug trafficking and similar activities generate huge unlawful profits.

Objective of Money Laundering : Criminals disguise sources, change the form, or move funds to avoid detection.

Need for AML Laws : AML laws prevent criminals from hiding illegally obtained money and protect the financial system.

FATF Formation : Anti-money laundering guidelines became globally relevant after the creation of FATF.

PMLA Objective : The Prevention of Money Laundering Act, 2002 aims to prevent money laundering and confiscate related property.

Stages of Money Laundering : The process involves Placement, Layering, and Integration.

Placement Stage : Illicit funds are introduced into the financial system.

Smurfing : Breaking large sums into small deposits below reporting thresholds.

Cash Smugglers : Criminals move cash across borders for foreign deposits.

Shell Companies : Inactive paper companies used to hide identity and movement of funds.

Layering Stage : Moving money through complex transactions to obscure its origin.

Chain-Hopping : Converting one digital currency into another across blockchains.

Mixing/Tumbling : Blending transactions across exchanges to hide the trail.

Cycling : Depositing fiat, buying/selling crypto, and withdrawing elsewhere.

Integration Stage : Illicit funds re-enter the legal economy appearing legitimate.

Fake Employees : Salaries paid to non-existent employees to withdraw illicit funds.

Loans to Directors : Non-repayable loans that help criminals extract illegal money.

Trade-Based ML : Laundering through misrepresentation of price, quantity, or quality in trade transactions.

Over/Under-Invoicing : Manipulation of invoice values to move illegal funds.

Multiple Invoicing : Using several invoices for the same goods/services to justify transfers.

False Description : Wrongly describing goods/services to disguise illicit transfers.

Global AML Framework : AML laws detect and report suspicious activity, tax evasion, and market manipulation.

Bank Secrecy Act (BSA) : US law requiring financial institutions to report large transactions and suspicious activity.

BSA Reporting : Financial institutions must keep records and file reports for cash transactions exceeding $10,000.

FinCEN Role : Administers BSA to safeguard the financial system from abuses.

FATF : Intergovernmental body formed in 1989 to set global AML standards.

FATF Recommendations : Forty recommendations revised periodically to combat evolving ML techniques.

India FATF Membership : India became a FATF member in 2010.

Mutual Evaluation : FATF reviews member countries' AML/CFT frameworks.

IMF AML Role : IMF helps maintain financial stability and provides AML/CFT policy guidance.

IMF Expansion : AML/CFT assessments became a regular part of IMF work after 2004.

BIS : Oldest international financial institution promoting monetary cooperation and AML guidelines.

BIS Guidelines : Provides risk-management guidelines for AML efforts.

Vienna Convention : 1988 convention requiring states to criminalize money laundering from drug trafficking.

International Cooperation : Convention promotes cooperation and extradition in ML investigations.

Bank Secrecy Limitation : Vienna Convention ensures secrecy laws do not hinder ML investigations.

UAPA Objective : Prevents unlawful and terrorist activities and allows banning and asset freezing.

Section 35 (UAPA) : Allows government to list terrorist organisations and amend schedules.

Section 51A (UAPA) : Allows freezing of funds and restricting entry/activities of listed individuals.

FEMA Purpose : Regulates foreign exchange transactions to prevent ML and terror financing.

PMLA Provisions : Requires record-keeping, reporting, and allows confiscation of proceeds of crime.

FIU-IND : Central agency receiving, analysing, and disseminating financial intelligence.

FIU Functions : Includes collecting CTRs, STRs, NTRs, CBWTRs, and sharing intelligence.

FINGate 2.0 Registration : Mandatory portal registration for all IFSCA regulated entities.

Designated Director Role : Oversees AML program compliance within a regulated entity.

AML & CFT Guidelines : Derived from PMLA, UAPA, and WMD Act for reporting and record-keeping.

WMD Act Section 12 : Prohibits knowingly facilitating restricted transactions related to weapons of mass destruction.

IFSC : Centres dealing with cross-border finance; India's GIFT IFSC established in 2015.

IFSCA : Unified regulator for banking, insurance, securities, and funds in IFSC.

IFSCA Guidelines : Ensures AML/CFT compliance and promotes ease of doing business.

Collective Action : Collaboration between institutions improves detection and prevention of terror financing.

Chapter-2 Prevention of Money Laundering Act, 2002 (PMLA)

Prevention of Money Laundering Act (PMLA) : Core legal framework to combat money laundering in India.

PMLA Objective : Prevents money laundering and enables confiscation of property derived from crime.

PMLA Enforcement Date : PMLA and PML Rules came into effect on 1 July 2005.

FIU-IND & Enforcement Directorate Powers : Both directors are granted exclusive and concurrent powers to enforce PMLA.

Reporting Entity Obligations : Banking companies and financial institutions must verify identity, maintain records, and report information to FIU-IND.

Section 2 Definitions : Defines key terms used throughout the PMLA.

Adjudicating Authority : Authority appointed under Section 6 to adjudicate matters under PMLA.

Appellate Tribunal : Established under Section 25 to hear appeals under PMLA.

Assistant Director : Officer appointed under Section 49 of PMLA.

Attachment : Prohibition on transferring or moving property involved in money laundering.

Authorised Person : Defined as per FEMA for foreign exchange related activities.

Banking Company : Any banking institution covered under the Banking Regulation Act.

Beneficial Owner : Individual who ultimately owns or controls a client of a reporting entity.

Client : Person engaged in a financial transaction with a reporting entity.

Corresponding Law : Foreign law corresponding to provisions of PMLA.

Dealer : Meaning as per Central Sales Tax Act.

Deputy Director : Officer appointed under Section 49.

Director / Additional Director / Joint Director : Senior officers empowered under Section 49.

Financial Institution : Includes NBFCs, chit funds, payment operators, housing finance companies.

Intermediary : Includes stockbrokers, merchant bankers, registrars, and other SEBI-regulated entities.

Investigation : Includes all proceedings to collect evidence under PMLA.

Money Laundering Definition : Defined under Section 3 as involvement in activities related to proceeds of crime.

Non-Banking Financial Company : Defined under RBI Act Section 45-I.

Offence of Cross-Border Implications : Involves crimes committed abroad whose proceeds are brought into India.

Payment System : Systems enabling clearing, settlement, or payment functions.

Payment System Operator : Entity operating a payment system, including overseas principals.

Person Definition : Includes individuals, HUFs, companies, firms, and artificial juridical persons.

Designated Business or Profession : Includes casinos, real estate agents, precious metal/stones dealers.

Precious Metal : Gold, silver, platinum, palladium, rhodium.

Precious Stone : Diamond, emerald, ruby, sapphire.

Proceeds of Crime : Property derived or obtained from criminal activity related to a scheduled offence.

Property Definition : Includes tangible, intangible, movable, immovable assets.

Reporting Entity : Banking companies, financial institutions, and intermediaries.

Scheduled Offence : Offences listed in Part A, B, and C of PMLA Schedule.

Special Court : Designated Court of Session under Section 43.

Transfer : Includes sale, mortgage, gift, pledge, or any transfer of rights.

Section 3 Offence of Money Laundering : Covers concealment, possession, acquisition, use, or projecting as untainted property.

Continuing Nature of ML : Money laundering continues as long as proceeds of crime are enjoyed.

Section 4 Punishment : Rigorous imprisonment of 3–7 years, extendable to 10 years for specific offences.

Section 5 Attachment of Property : Allows provisional attachment of property for up to 180 days.

Section 12 Record Maintenance : Reporting entities must maintain records and identity documents for five years.

Rule 3 PML Rules : Specifies types of transactions required to be reported to FIU-IND.

Cash Transactions Reporting : Cash transactions above ₹10 lakh or structured transactions crossing ₹10 lakh.

NPO Transactions Reporting : NPO receipts exceeding ₹10 lakh.

Suspicious Transaction Reporting : Reports must be made within 7 working days upon identifying suspicion.

Cross-Border Wire Transfers : Transfers exceeding ₹5 lakh must be reported.

Immovable Property Reporting : Purchase/sale of property worth ₹50 lakh or more must be reported quarterly.

Principal Officer : Officer responsible for reporting and coordinating PMLA compliance.

Designated Director : Person ensuring overall compliance under Chapter IV of PMLA.

IFSCA Compliance Requirements : Entities must conduct risk assessments, monitor transactions, follow KYC norms.

Main Investigating Authorities : Include Directorate of Enforcement, FIU-IND, Adjudicating Authority, and other regulators.

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

PMLR Purpose : Rules created to implement PMLA by defining procedures for maintenance of records and client verification.

Rule-Making Power : Central Government framed rules under Section 73 of PMLA.

2023 Amendment : Rules amended via notification dated 7 March 2023.

Internal Controls : Reporting entities must develop policies, systems and controls to prevent financial crimes.

Customer Due Diligence : Entities must verify customers before onboarding or executing transactions.

Suspicious Activity Reporting : Mandatory reporting of suspicious transactions to authorities.

Client Identity Records : Identity records must be kept for ten years after relationship ends.

Rule 3 Scope : Defines nature and value of transactions to be recorded.

Cash Transaction Rule : Cash transactions above ₹10 lakh must be recorded.

Structured Transactions : Series of connected transactions exceeding ₹10 lakh must be monitored.

NPO Receipts : NPO transactions above ₹10 lakh must be recorded.

Forged Currency Transactions : Transactions involving counterfeit currency must be reported.

Suspicious Transactions : Covers all suspicious deposits, withdrawals, transfers, or credits.

Non-Monetary Accounts : Suspicious activity in demat or securities accounts must be tracked.

Money Transfers : Includes domestic and international transfers for clients and non-clients.

Loans & Advances : Covers credit substitutes, investments, bills, and derivatives.

Collection Services : All collection of cheques and instruments must be recorded.

Cross-Border Transfers : Transfers above ₹5 lakh must be reported.

Immovable Property Reporting : Property transactions above ₹50 lakh must be recorded.

Rule 3A Group Policies : Groups must implement global AML/CFT policies and safeguard information.

Rule 4 Transaction Records : Records must permit reconstruction of each transaction.

Rule 5 Internal Mechanism : Entities must maintain information as required by regulators.

Rule 7 Designated Officer : Principal Officer must report transactions to Director FIU-IND.

Internal Detection Mechanism : Entities must develop systems to detect Rule 3 transactions.

Rule 8 Reporting Timelines : Monthly reports due by 15th; STRs within 7 days.

Delay Penalties : Each day of delay counts as a separate violation.

Rule 9 Client Due Diligence : CDD must be completed at onboarding and during specific transactions.

Beneficial Owner Identification : Entities must identify beneficial owners for all clients.

BO for Companies : Natural person with more than 10% ownership or control.

BO for Partnerships : Person holding more than 10% capital or profits.

BO for Associations : Person holding more than 15% interest.

Senior Managing Official : Acts as BO when no natural person identified.

BO for Trusts : Includes settlor, trustees, beneficiaries with 10%+ interest.

Exemption for Listed Entities : BO identification not needed for listed companies.

KYC Records Registry : CKYC processes and stores client KYC records.

KYC Identifier : Unique number issued after CKYC record processing.

KYC Retrieval : Entities retrieve KYC using KYC Identifier without re-collection.

Third-Party CDD : Permitted if third party is regulated and compliant.

Small Accounts : Can be opened with minimal documents but with strict monitoring.

Company Documents : Includes incorporation documents, PAN, resolutions, and authorised signatories.

Partnership Documents : Includes registration, deed, PAN, and authorised signatories.

Trust Documents : Includes registration, deed, PAN, trustees, and beneficiaries.

Unincorporated Bodies : Must submit resolutions, PAN, and proof of existence.

NPO Registration Requirement : NPOs must be registered on DARPAN portal.

Record Updating Requirement : Clients must update documents within 30 days of changes.

Prohibition on Anonymous Accounts : No fictitious or anonymous accounts allowed.

Ongoing Due Diligence : Continuous monitoring of client transactions and risk.

Risk Assessment Requirement : Entities must document risk assessment and keep it updated.

Digital KYC Requirements : Live photo, document scan, watermarking and OTP verification required.

Application Controls : KYC application must be secure and used only by authorised staff.

CAF Verification : All data must match documents; CAF digitally signed upon verification.

Chapter-4 Scheduled Offences

Scheduled Offence : An offence listed in Parts A, B, or C of the PMLA Schedule that generates proceeds of crime.

Foundation of ML Offence : Money laundering arises only when a scheduled offence has been committed.

Section 2(1)(y) PMLA : Defines scheduled offences covered under the Act.

Parts A, B, C of Schedule : Contain offences from IPC/BNS and various other laws linked to money laundering.

Part A (No Threshold) : Covers major offences from IPC/BNS, NDPS Act, UAPA, Arms Act, etc.

Part B (Threshold) : Includes Customs Act offences with monetary threshold of ₹3M or ₹10M.

Part C (Cross-Border) : Covers Part A offences when having cross-border implications.

Proceeds of Crime : Property derived from any scheduled offence.

Criminal Conspiracy : IPC 120B / BNS 61(2) classified as a scheduled offence.

Waging War : IPC 121 / BNS 147 includes offences against the State.

Conspiracy Against State : IPC 121A / BNS 148 considered scheduled offence.

Counterfeiting Govt Stamp : IPC 255–260 / BNS equivalents listed under scheduled offences.

Murder : IPC 302 / BNS 103(1) listed under Part A.

Culpable Homicide : IPC 304 / BNS 105 included in scheduled offences.

Attempt to Murder : IPC 307 / BNS 109 recognised under Part A.

Kidnapping for Ransom : IPC 364A / BNS 140(2) included as scheduled offence.

Extortion : IPC 384–389 / BNS 308 covered under scheduled offences.

Robbery & Dacoity : IPC 392–402 / BNS 310–313 included in Part A.

Receiving Stolen Property : IPC 411–414 / BNS 317 series listed in Schedule.

Cheating : IPC 417–420 / BNS 318–320 included in scheduled offences.

Fraudulent Transfers : IPC 421–424 / BNS 320–323 covered as scheduled offences.

Forgery : IPC 467–476 / BNS 338–342 recognised under Part A.

Counterfeit Property Marks : IPC 481–488 / BNS 345–350 included in Part A.

Fake Currency Offences : IPC 489A–489B listed as serious scheduled offences.

NDPS Violations : Offences under NDPS Act Sections 15–29 are included in Part A.

NDPS Import/Export Offence : Section 23 includes cross-border narcotic trafficking.

Financing Illicit Traffic : NDPS Section 27A is a major scheduled offence.

Explosive Substances Act : Sections 3–5 included for offences involving explosives.

UAPA Terror Offences : Sections 10–40 cover terrorism-related scheduled offences.

Terrorist Financing : UAPA Section 17 included under Part A.

Arms Act Violations : Sections 25–30 relating to prohibited arms are scheduled offences.

Wildlife Protection Act : Section 51 with various clause violations included in Part A.

Immoral Traffic Act : Sections 5–9 included as scheduled offences.

Prevention of Corruption Act : Sections 7–13 involving public servant corruption included.

Explosives Act : Section 9B and 9C relating to explosive misuse listed under Part A.

Antiquities Act Violations : Sections 25 and 28 included for illegal antiquities trade.

SEBI Act Offences : Section 12A and 24 for securities manipulation are scheduled offences.

Customs Act Evasion : Section 135 covered in Part A & B depending on threshold.

Bonded Labour Act : Sections 16, 18, 20 included as scheduled offences.

Child Labour Offence : Section 14 included under Part A.

Human Organs Act : Sections 18–20 for illegal organ trade included.

Juvenile Justice Act : Sections 23–26 included for offences involving juveniles.

Foreigners Act Violations : Sections 14–14C included as scheduled offences.

Passport Act Violations : Section 12 included for misuse of passport.

Copyright Violations : Sections 63–68A included in Part A.

Trademark Offences : Sections 103–120 regarding counterfeit trademarks included.

IT Act Offence : Section 72 on breach of confidentiality listed in Schedule.

Environmental Offences : Offences under Water, Air, and Environment Acts included.

Companies Act Fraud : Section 447 recognised as a scheduled offence.

Cross-Border Implication : Any Part A offence involving cross-border transactions falls in Part C.

Chapter-5 IFSCA (AML, CFT & KYC) Guidelines, 2022

IFSCA Guidelines 2022 : Framework governing AML, CFT and KYC compliance for regulated entities.

Regulated Entity (RE) : Any unit licensed, registered or authorised by IFSCA.

AML-CFT Policy : A mandatory policy approved by Governing Body outlining AML and CFT controls.

KYC Policy : Forms part of the RE's AML-CFT policy and outlines customer verification norms.

Senior Management Responsibility : They must ensure compliance with the AML/CFT guidelines.

Risk-Based Approach (RBA) : Method to identify and assess ML/TF risks depending on business nature.

Objective & Proportionate RBA : RBA must be based on reasonable grounds and proportional to risk.

Periodic RBA Review : RBA must be reviewed at least once in two years or when trigger events occur.

Enterprise-Wide Risk Assessment : RE must assess ML/TF risks across all business units and channels.

Risk Classification : Classify ML/TF risk as low, medium, or high for applying mitigation measures.

RBA Documentation : Record risk assessment, system implementation and controls for ML/TF risks.

Authority Access : Risk assessment records must be made available to IFSCA upon request.

Business Risk Assessment : Assessment based on size, complexity, customer type and activities.

Customer-Type Risk : Risk arising from customer activities and profiles.

Geographical Risk : Risk due to exposure to certain countries or jurisdictions.

Product/Service Risk : Risk based on the nature of products, services, and delivery channels.

Transaction Complexity Risk : Risk from volume and complexity of customer transactions.

New Product Risk : New technologies and practices must undergo ML/TF risk assessment.

Technology Risk : Risk linked to new tech used for products or delivery mechanisms.

Mitigation Measures : RE must apply risk-based mitigation controls.

AML/CFT System Controls : Policies, procedures and systems tailored to identified risks.

Senior Management Review : AML systems must allow periodic review by management.

PEP Identification : System must detect whether a customer/beneficial owner is a PEP.

Compliance with Laws : Systems must support compliance with AML/CFT legislations.

Ongoing System Assessment : AML systems must be periodically reviewed for adequacy.

Senior Management Approval : AML/CFT controls must be approved at senior level.

Suspicious Transaction Indicators : Detect indicators, ask questions, review records, evaluate findings.

Internal Reporting Duties : Employees must promptly notify Principal Officer of suspicious cases.

Principal Officer Notification : All suspicion details must be escalated internally.

STR Reporting : Suspicious Transaction Reports must be filed promptly to FIU-IND.

Use of FIU Utilities : REs must use reporting formats and utilities prescribed by FIU-IND.

Delay as Violation : Daily delay in filing reports constitutes separate violations.

NTR Filing : NPO Transaction Reports must be filed by 15th of next month.

Confidentiality of STR : REs and employees must maintain secrecy of STR filings.

Professional Reporting Obligation : Lawyers, notaries and accountants must file STRs in specified cases.

Correspondent Banking Policy : Requires governing body approval and risk-based assessment.

Respondent Bank Assessment : Verify respondent bank's management, activities and jurisdiction.

AML Controls of Respondent Bank : Ascertain adequacy of AML/CFT controls before establishing ties.

No Shell Institutions : Correspondent banking cannot be done with shell banks.

High-Risk Jurisdiction Caution : Extra caution required with banks in FATF-deficient countries.

Wire Transfer Identification : Ordering bank must verify originator identity before transfer.

High-Risk Transaction Monitoring : Screen transactions involving sanctioned or high-risk countries.

Terrorist Name Screening : Block or freeze assets if originator/beneficiary matches terror list.

Cross-Border Transfer Requirements : Must include originator and beneficiary details in messages.

USD 1000 Threshold Rules : Additional data required for transfers above USD 1000.

Batch Transfer Requirements : Complete traceable originator/beneficiary information must exist.

Internal Policies : Policies must guide employees and be updated for emerging risks.

Compliance Function : Principal Officer must oversee AML compliance with proper authority.

Independent Audit : RE must maintain an independent audit to examine AML effectiveness.

Training Requirements : Employees must be trained to detect, understand and respond to ML/TF risks.

Record Keeping Requirement : CDD, business records, STRs and analysis must be preserved for six years.

Chapter-6 IFSCA Guidelines for KYC Norms

IFSCA KYC Guidelines : Apply to every Regulated Entity and relevant financial groups.

Customer Risk Management : Risk assessment determines risk rating as high, medium, or low.

Customer Risk Assessment : Must be completed before CDD for new and sometimes existing customers.

Identify Customer & BO : RE must identify customer and beneficial owner before onboarding.

Purpose of Relationship : Obtain details on intended nature and purpose of account relationship.

Customer Background Factors : Consider business type, ownership structure, residence, product usage.

High-Risk Customer Indicators : Include complex ownership, nominee shareholders, unusual relationships.

High-Risk Country Indicators : Countries with corruption, terrorism financing, weak AML laws.

High-Risk Product Indicators : Private banking, anonymity services, non-face-to-face dealings.

Low-Risk Customer Indicators : Government entities, listed companies, regulated foreign institutions.

Low-Risk Product Indicators : Non-life insurance, pension schemes without surrender value.

Prohibited Relationships : No onboarding of anonymous accounts, shell institutions or unverifiable BOs.

Customer Due Diligence (CDD) : Includes CDD, Enhanced CDD, and Simplified CDD based on risk rating.

Enhanced CDD : Required for high-risk customers with deeper verification.

Simplified CDD : Permitted only for low-risk customers with limited verification.

Timing of CDD : Conducted at onboarding and during ongoing monitoring or when suspicion arises.

Pre-verification Relationship : Allowed if low risk and verification completed within 30 business days.

Failure to Verify : Relationship suspended at 30 days and terminated at 120 days.

CDD Measures : Verify identity, understand purpose, monitor transactions continuously.

Natural Person Information : Collect name, ID, DOB, address, nationality, contact details.

Legal Person Information : Collect name, registration details, address, incorporation documents.

Connected Parties : Identify and verify individuals linked to legal persons.

Verification Standards : Use reliable independent sources; government IDs preferred.

V-CIP Onboarding : Video KYC allowed for individuals, proprietors, BOs and signatories.

Digital KYC Requirements : Aadhaar, PAN and additional documents as required by RE.

Authorised Persons Verification : Identify and verify individuals acting on behalf of customers.

BO Identification Requirements : Identify persons owning/control over 25% companies, 15% partnerships/associations.

Trust BO Requirements : Identify settlor, trustee, beneficiaries with 15%+ interest.

Listed Company Exemption : No beneficial owner verification required unless suspicion arises.

Life Insurance Beneficiary CDD : Obtain beneficiary name or details sufficient for later identification.

Purpose of Business Relationship : Understand customer's intent proportionate to risk profile.

PEP Identification : Systems must identify customers, BOs, and beneficiaries who are PEPs.

PEP Enhanced Measures : Verify identity, source of wealth, senior management approval required.

PEP Ongoing Monitoring : Higher monitoring frequency due to elevated risk.

Enhanced Monitoring Requirements : More frequent reviews and deeper transaction scrutiny.

First Payment Rule : First payment must come from an account in customer's name in regulated institution.

Simplified CDD Restrictions : Cannot be used if ML/TF suspicion exists.

Ongoing Monitoring : Scrutinise unusual, large or complex transactions; update information regularly.

Risk Rating Review : Reassess customer risk when circumstances change.

Sanction Screening : Screen all customers and transactions against UNSC and other sanctions lists.

Failure to Complete CDD : RE must not open accounts and may need to report STR.

Periodic Updation : High risk yearly, medium risk every 3 years, low risk every 5 years.

Address Change Verification : Self-declaration plus confirmation within two months.

Non-Natural Persons Updation : Self-declaration and updated BO information required.

Expired Documents : Fresh CDD required if documents have expired.

PAN Verification : PAN must be verified from issuing authority database during updation.

Customer Acknowledgment : RE must issue acknowledgment for documents received.

Facility for Updation : REs should allow periodic updation at branches or digital channels.

IFSCA vs Other Regulators : IFSCA guidelines emphasise global AML/CFT alignment and cross-border risks.

International Requirements : Greater focus on global sanctions, international clients and FATF compliance.

Chapter-7 PMLA Case Studies

Case Study Purpose : Chapter demonstrates practical implementation of PMLA through real FIU-IND and IFSCA orders.

FIU-IND Authority : FIU-IND exercises powers under Section 13(2)(d) of PMLA to impose penalties.

VDA SP Classification : Virtual Digital Asset Service Providers are 'reporting entities' under Section 2(1)(wa) of PMLA.

Bybit Violation – No Registration : Bybit expanded services without mandatory FIU-IND registration.

Blocking of Bybit Services : FIU-IND blocked Bybit's websites through MEITY for persistent non-compliance.

AML/CFT Guidelines for VDA SP : FIU-IND issued guidelines for VDA entities on March 10, 2023.

Registration Circular for VDA SP : Issued by FIU-IND on October 17, 2023.

Bybit Penalty : FIU-IND imposed ₹9.27 crore penalty on Bybit.

Bybit Rule Violations : Violated Section 12(1), Rule 2(1)(h), Rule 7(2), Rule 8(2), Rule 8(4), Rule 3(1)(D), Rule 7(3).

Non-compliance Impact : Repeated non-compliance triggered strong regulatory actions.

PIBPL Classification : Prowess Insurance Brokers Pvt. Ltd. registered as a Direct Broker with IRDAI.

PIBPL IFSC Branch Approval : Approved under IRDAI IIIO Guidelines 2019 for GIFT-IFSC operations.

Approval Validity Issue : IFSC branch authorization expired with CoR on September 21, 2021.

Requirement to Renew CoR : PIBPL required to renew CoR with IRDAI before IFSCA approval.

IFSCA Direction to PIBPL : Directed in Jan 2022 not to engage in new business until renewal.

Violation by PIBPL : Continued operations despite IFSCA directive.

Non-Acknowledgement Issue : PIBPL did not acknowledge the IFSCA communication.

Information Request Non-compliance : IFSCA requested operational details on May 30, 2023.

Main Issue in PIBPL Case : Failure to comply with regulatory directions under IIIO Regulations 2021.

PIBPL Order : IFSCA cancelled approval for operating as IFSC Insurance Intermediary Office.

Post-Cancellation Liability : PIBPL remains liable for dues, fees, and record maintenance.

Neo Asset Management Registration : Registered as FME (Non-Retail) on Nov 22, 2023.

Surprise Visit Findings : Principal Officer and Key Managerial Personnel absent during two inspections.

IFSCA Advisory Letter : Issued on Sept 12, 2024 directing compliance.

Failure to Acknowledge Advisory : Neo did not acknowledge advisory letter or collect hard copy.

Third & Fourth Visits : On Oct 17 & 24, 2024, office again found non-operational.

Non-Compliance Issue Neo : Repeated absence of mandatory officers violated Fund Management Regulations.

Warning Issued to Neo : IFSCA issued warning under Regulation 143 & Section 13 of IFSCA Act.

Future Action Warning : Repeated violations will trigger stringent regulatory action.

Way2Wealth Case Trigger : Case initiated based on SEBI reference alleging PMLA non-compliance.

AML Monitoring Failure : Failed to raise or investigate alerts and file STRs.

Failure to Consider SEBI Orders : Adverse SEBI orders were ignored during AML monitoring.

Way2Wealth Penalty : FIU-IND imposed ₹1 lakh penalty.

Corrective Directions : Directed to implement corrective actions under Sections 13(2)(a) & 13(2)(b).

Certification Requirement : Designated Director and Principal Officer required to certify compliance.

Paytm Payments Bank Reporting Entity : Classified as reporting entity under Section 2(1)(wa).

Law Enforcement FIRs : FIRs revealed online gambling and fraud networks using bank accounts.

Routing of Proceeds : Illegal proceeds routed through Paytm Payments Bank accounts.

Fraudulent Services : Entities offered gambling, dating, streaming; proceeds remitted abroad.

Payout Service Deficiency : Bank lacked mechanisms to detect suspicious activity in payout services.

Third-Party KYC Failure : Relied on non-compliant third-party KYC provider.

Failure to File STRs : Did not file STRs for 34 beneficiary accounts.

Due Diligence Failure : Failed to perform ongoing due diligence on high-risk beneficiary accounts.

Paytm Violations : Breached obligations under Section 12(1) and Rules 3, 7, 8, 9.

Paytm Penalty : FIU-IND imposed ₹5.49 crore fine.

Regulatory Objective : To protect financial system from misuse by high-risk or illegal entities.

Importance of AML Controls : Cases highlight need for strong monitoring and KYC systems.

Importance of Timely Registration : Entities must secure registration before operating.

Role of Surprise Visits : Used by IFSCA to verify compliance readiness.

Adjudicating Powers : FIU-IND & IFSCA may impose penalties, warnings, or cancel approvals.

Chapter-8 FATF, AML/CFT Standards & Trade-Based Money

FATF Purpose : Leads global action against money laundering, terrorist financing and proliferation financing.

FATF Membership : Over 200 countries committed to implementing FATF Standards.

FATF Plenary : Decision-making body meeting three times per year to review compliance.

Grey List : Jurisdictions under increased monitoring to fix strategic deficiencies.

Black List : High-risk jurisdictions subject to counter-measures by FATF members.

FATF President Role : Chairs FATF Plenary, spokesperson, oversees FATF Secretariat.

Current FATF President : Elisa de Anda Madrazo (Mexico), term 1 July 2024–30 June 2026.

FATF Vice-President : Giles Thomson (United Kingdom), from July 1, 2025.

FATF Mandate : Open-ended mandate since 2019 to counter ML/TF/PF threats.

2001 Mandate Expansion : FATF mandate expanded to include combating terrorist financing.

FATF Recommendations : Comprehensive AML/CFT framework of 40 Recommendations.

Seven Areas of FATF Standards : Policies, ML & confiscation, TF/PF, preventive measures, transparency, institutional powers, international cooperation.

Risk-Based Approach : Countries must assess and mitigate ML/TF risks based on national context.

Recommendation 1 : Assess risks and apply a risk-based approach.

Recommendation 2 : National cooperation and coordination.

Money Laundering Offence : Recommendation 3 covers ML offence requirements.

Confiscation Measures : Recommendation 4 covers freezing and confiscation powers.

Terrorist Financing Offence : Recommendation 5 requires criminalising TF.

Targeted Financial Sanctions : Recommendations 6 & 7 for sanctions on terrorism & proliferation.

NPO Vulnerability : Recommendation 8 highlights NPO risk of TF misuse.

Customer Due Diligence : Recommendation 10 outlines CDD requirements.

Record Keeping : Recommendation 11 mandates maintenance of transaction records.

PEP Measures : Recommendation 12 requires enhanced checks for politically exposed persons.

Correspondent Banking Controls : Recommendation 13 emphasises due diligence for correspondent relationships.

Money or Value Transfer Services : Recommendation 14 requires licensing MVTS.

New Technologies Risk : Recommendation 15 requires assessing ML/TF risk in fintech innovations.

Payment Transparency : Recommendation 16 covers wire transfer originator/beneficiary details.

Third-Party Reliance Rules : Recommendation 17 controls reliance on third-party CDD.

Internal Controls : Recommendation 18 mandates AML programs for financial groups.

High-Risk Countries : Recommendation 19 requires enhanced due diligence for such countries.

STR Reporting : Recommendation 20 requires reporting suspicious transactions.

Tipping-off Prohibition : Recommendation 21 prevents disclosure of STR filings.

DNFBP CDD : Recommendations 22 & 23 impose AML duties on lawyers, accountants, real-estate etc.

Beneficial Ownership (Legal Persons) : Recommendation 24 requires transparency of company ownership.

Beneficial Ownership (Legal Arrangements) : Recommendation 25 requires transparency in trusts.

Regulation of Financial Institutions : Recommendation 26 sets supervision requirements.

Powers of Supervisors : Recommendation 27 provides authority to enforce AML rules.

DNFBP Supervision : Recommendation 28 supervises non-financial professions.

Role of FIUs : Recommendation 29 mandates creation of national FIU.

Law Enforcement Responsibilities : Recommendation 30 requires investigative authorities to tackle ML/TF.

FIU & Law Enforcement Powers : Recommendation 31 outlines investigative powers.

Cash Couriers Control : Recommendation 32 requires measures to detect cross-border cash movement.

Statistics Requirement : Recommendation 33 requires data collection on AML effectiveness.

Guidance & Feedback : Recommendation 34 requires regulators to issue AML guidance.

Sanctions Requirement : Recommendation 35 mandates effective and dissuasive AML sanctions.

International Instruments : Recommendation 36 requires adherence to UN AML/TF conventions.

Mutual Legal Assistance : Recommendation 37 enables cross-border cooperation.

Freezing & Confiscation Assistance : Recommendation 38 mandates cooperation in freezing criminal assets.

Extradition Requirements : Recommendation 39 encourages extradition for ML/TF crimes.

Other International Cooperation : Recommendation 40 supporting cross-border intelligence sharing.

Trade-Based ML Definition : Disguising proceeds of crime using trade transactions to move value.

Three Movement Methods : Financial system, physical cash movement, and trade misrepresentation.

International Trade Vulnerabilities : Huge volume, complex financing, weak customs verification, limited inspection.

Basic TBML Techniques : Over/under-invoicing, multiple invoicing, over/under-shipment, false description.

Complex TBML – Black Market Peso Exchange : Combines multiple ML techniques without exporter–importer collusion.

Strengthening TBML Controls : Better awareness, domestic information sharing, improved international cooperation.

==========

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.

NISM IFSCA 01 October - 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