NISM CERTIFICATION EXAMINATION WORK BOOK

NISM-IFSCA-01

Anti Money Laundering and Counter Terrorist Financing in the IFSC

National Institute of Securities Markets

A Capacity Building Initiative of SEBI

Workbook for NISM-IFSCA-01:

Certification Course on Anti Money Laundering and Counter Terrorist Financing in the IFSC

National Institute of Securities Markets
www.nism.ac.in

This workbook has been developed to assist candidates preparing for the NISM-IFSCA-01: Certification Course on Anti Money Laundering and Counter Terrorist Financing in the IFSC.

Workbook Version: December 2025[1]

Published by:
National Institute of Securities Markets

NISM Registered Office
5th floor, NCL Cooperative Society,
Plot No. C-6, E-Block, Bandra Kurla Complex,
Bandra East, Mumbai, 400051

National Institute of Securities Markets
Patalganga Campus
Plot IS-1 & IS-2, Patalganga Industrial Area
Village Mohopada (Wasambe)
Taluka-Khalapur
District Raigad-410222.

Website: www.nism.ac.in

[1]Note: This is the revised workbook (version December 2025). Kindly refer to the workbook (version: December 2025) for appearing in the NISM Series XV: Research Analyst Certification Examination on or after January 30, 2026.

Foreword

NISM is a leading provider of high-end professional education, certifications, training and research in financial markets. NISM engages in capacity building among stakeholders in the securities markets, through professional education, financial literacy, enhancing governance standards and fostering policy research.

The NISM certification programs aim at enhancing the quality and standards of professionals employed in various segments of the financial sector. NISM develops and conducts certification examinations and Continuing Professional Education (CPE) programs that aim at ensuring that professionals meet the defined minimum common knowledge benchmark for various critical securities market functions.

NISM certification examinations and educational programs primarily serve different securities market intermediaries focusing on varied product lines and functional areas. NISM certifications have established knowledge benchmarks for various market products and functions such as equities, mutual funds, derivatives, compliance, operations, advisory and research. NISM certification examinations and training programs provide a structured learning plan and career path to students and job aspirants, wishing to make a professional career in the securities markets.

NISM supports candidates by providing lucid and focused workbooks that assist them in understanding the subject and preparing for NISM Examinations. This book covers important topics to create awareness among the capital market intermediaries operating in the IFSCA ecosystem. The book focusses on discussing various regulatory aspects of prevention of money laundering. It discusses the concepts such as AML, CFT, PF, scheduled offences, regulatory provisions/guidelines of AML, CFT and KYC under the PMLA, IFSCA AML, CFT and KYC Guidelines, among others. It also provides learners the practical understanding on the implementation and coverage of PMLA through different case studies.

Sashi Krishnan

Director

Disclaimer

The contents of this publication do not necessarily constitute or imply its endorsement, recommendation, or favoring by the National Institute of Securities Markets (NISM) or the International Financial Services Authority (IFSCA). This publication is meant for general reading and educational purpose only.

The statements/explanations/concepts are of general nature and may not have taken into account the particular objective/ move/ aim/ need/ circumstances of individual user/ reader/ organization/ institute. Thus, NISM and IFSCA do not assume any responsibility for any wrong move or action taken based on the information available in this publication.

Therefore, before acting on or following the steps suggested on any theme or before following any recommendation given in this publication user/reader should consider/seek professional advice.

The publication contains information, statements, opinions, statistics and materials that have been obtained from sources believed to be reliable and the publishers of this title have made best efforts to avoid any errors. However, publishers of this material offer no guarantees and warranties of any kind to the readers/users of the information contained in this publication.

Since the work and research is still going on in all these knowledge streams, NISM and IFSCA do not warrant the totality and absolute accuracy, adequacy or completeness of this information and material and expressly disclaim any liability for errors or omissions in this information and material herein. NISM and IFSCA do not accept any legal liability whatsoever based on any information contained herein.

While the NISM Certification examination will be largely based on material in this workbook, NISM does not guarantee that all questions in the examination will be from material covered herein.

Acknowledgement

This workbook has been developed jointly by the Certification Team of National Institute of Securities Markets (NISM) and NISM Subject Matter Expert—Ms. Monica Sachdeva. We draw our sincere gratitude towards IFSCA, for their efforts in reviewing the workbook.

About the Certification Examination – NISM-IFSCA-01: Certification Course on Anti Money Laundering and Counter Terrorist Financing in the IFSC

The examination seeks to create a common minimum knowledge benchmark for the capital market intermediaries about Anti Money Laundering (AML) and Counter Terrorist Financing regulations in IFSC ecosystem.

The examination covers various aspects related to Anti Money Laundering (AML), Counter-Terrorist Financing (CFT) and Know Your Customer. Some of them are the Prevention of Money Laundering Act, 2002 (PMLA), Scheduled Offences, AML, CFT and KYC Guidelines and PMLA related cases.

The certification aims to create awareness among the capital market intermediaries about the AML and CFT regulations in IFSC ecosystem.

Examination Objectives

On successful completion of the examination, the candidate should:

- Know the concepts of AML and CFT and related aspects, provisions of the PMLA, and scheduled offences;
- Understand guidelines pertaining to Anti Money Laundering (AML) Standards, Combating the Financing of Terrorism (CFT) and Proliferation Financing (PF),
- Understand the IFSCA Anti Money Laundering, Counter Terrorist-Financing and Know Your Customer Guidelines, 2022 from Regulated Entities' perspective.
- Know about the Financial Action Task Force and its recommendations for AML and CFT.

Assessment Structure

1. The examination consists of 50 questions of 1 mark each and should be completed in 1 hour.
2. The passing percentage for the examination is 50 percent (25 marks).
3. There shall be no negative marking.

How to register and take the examination

To find out more and register for the examination please visit: www.nism.ac.in
For any feedback and/or queries, please write back at certification@nism.ac.in

Syllabus Outline with Weightages

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**

Contents

Part A: General Rules and Regulations related to Anti-Money Laundering in India

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

Learning Objective- After studying this chapter, you should know about:

- Detailed concept of Money Laundering and Combating the Financing of Terrorism
- Global and Indian Initiatives to combat money laundering

1.1. Introduction to the concept of money laundering

A large number of criminal acts aim to generate a profit for the individual or group that carries out the act. Money laundering is the process of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardizing their source. Illegal arms sales, smuggling, and the activities of organised crime, including drug trafficking and prostitution rings, can generate huge amounts of proceeds. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to "legitimize" the ill-gotten gains through money laundering.[2]

When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention. Practice of or engagement in any of such activities is known as Money Laundering.

1.1.1 Need for Anti Money Laundering Laws (History)

Anti-money laundering (AML) laws are important and much required because they help preventing criminals from hiding illegally obtained money and the financial impact of money laundering on a country, thus safeguarding the financial system from crimes.

Anti-money laundering guidelines came into prominence globally as a result of the formation of the Financial Action Task Force (FATF) and the promulgation of an international framework of anti-money laundering standards. These standards began to have more relevance in 2000 and 2001, after FATF began a process to publicly identify countries that were deficient in their anti-money laundering laws and international cooperation.

[2] https://fiuindia.gov.in/files/FAQs/faqs.html

The Prevention of Money Laundering Act, 2002 (PMLA) forms the core of the legal framework put in place by India to combat money laundering. The provisions of PMLA came into force on July 1, 2005. The objective of PMLA is, "to prevent money-laundering and to provide for confiscation of property derived from, or involved in, money-laundering and for matters connected therewith or incidental thereto."

1.2. Process of Money Laundering

There are typically three stages[3] of the money laundering process to release laundered funds into the legal financial system. These three stages of money laundering are:

- Placement
- Layering
- Integration/extraction

1.2.1 Money laundering Stages

Stage 1: Placement in the financial system

The placement stage in money laundering is when the illegally obtained funds are introduced in the financial system. This is often done by breaking up large amounts of cash into less conspicuous smaller sums to deposit directly into a bank account or by purchasing monetary instruments such as checks or money orders that are collected and deposited into accounts at other locations. The placement stage of money laundering is full of challenges for the criminals as it involves placing money into the legal system without causing any suspicion.

Some placement methods include:

- **Adding illicit cash:** Adding illicit cash from a crime to the legitimate takings of a business, particularly those with little or no variable costs;
- **Smurfing:** Smurfing is where small amounts of money below the AML reporting threshold are inserted into bank accounts or credit cards and used to pay expenses, etc.;
- **Mules[4] or cash smugglers:** Cash is smuggled across borders and deposited into foreign accounts;
- **Hiding Identity:** Hiding the beneficial owner's identity through trusts and offshore companies;
- **Investing in commodities:** Using gems and gold that can be moved easily to other jurisdictions;

[3]https://complyadvantage.com/insights/3-stages-money-laundering/

[4]As per SEBI PFUTP Regulations, "mule account" includes a trading account maintained with a stock broker or a dematerialised account or bank account linked with such trading account in the name(s) of a person, where the account is effectively controlled by another person, whether or not the consideration for transactions in the account are paid by such other person.

- **Buying and Selling:** Using cash for quick turnaround investment in assets such as real estate, cars, and boats;
- **Gambling:** Using casino transactions to launder money
- **Shell companies:** Establishing inactive companies or corporations that exist only on paper.

Stage 2: Layering the funds

The layering stage is when the launderer moves the money through a series of financial transactions with the goal of making it difficult to trace the original source.

The funds could be channeled through the purchase and sales of investments, a holding company, or simply moved through a series of accounts at banks around the globe. Widely scattered accounts are most likely to be found in jurisdictions that do not cooperate with AML investigations. In some instances, the launderer could disguise the transfers as payments for goods or services or as a private loan to another company, giving them a legitimate appearance. Few layering tactics are:

- **Chain-hopping** — converting one digital currency into another and moving from one blockchain to another;
- **Mixing or tumbling** — the blending of various transactions across several exchanges, making transactions harder to trace back to a specific exchange, account, or owner;
- **Cycling** —making deposits of fiat currency from one bank, purchasing and selling digital currency, and then depositing the proceeds into a different bank or account.

Stage 3: Integration into the legitimate financial system

The integration stage of money laundering is the final step in the laundering process. This is when the launderer attempts to integrate illicitly obtained funds into the legitimate financial system. To use the funds to buy goods and services without attracting attention from law enforcement or the tax authorities, the criminal may invest in real estate, luxury assets, or business ventures.

They are often content to use payroll and other taxes to make the "washing" more legitimate, accepting a 50% "shrinkage" in the wash as the cost of doing business.

Common integration tactics include:

- Fake employees – a way of getting the money back out. Usually paid in cash and collected;
- Loans – to directors or shareholders, which will never be repaid;
- Dividends – paid to shareholders of companies controlled by criminals.

While not all money laundering cases will use all the three-stage process – they could be combined or stages repeated several times, thus the rule of three stages of money laundering frames the thinking of many compliance teams.

1.2.2 Basic Trade-Based Money Laundering Techniques

For the purpose of this study, trade-based money laundering is defined as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origin. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports. In many cases, this can also involve abuse of the financial system through fraudulent transactions involving a range of money transmission instruments, such as wire transfers. The basic techniques of trade-based money laundering include:

- over- and under-invoicing of goods and services;
- multiple invoicing of goods and services;
- over- and under-shipments of goods and services; and
- falsely described goods and services.

However, it may be noted that all of these techniques are not necessarily in use in every country[5].

1.3. Global initiatives towards Anti Money Laundering Laws

Anti-money laundering Laws are an international web of laws, activities, regulations, and procedures, aimed at uncovering money that has been disguised as legitimate income. For decades, governments and law enforcement agencies have tried to fight crime by following the money, thus aiming to achieve the purpose of the AML Laws which is to help detect and report suspicious activity including the predicate offenses to money laundering and terrorist financing, securities fraud and market manipulation.

Let’s understand few Global Initiatives towards AML proceeds by understanding these Laws:

1.3.1 Bank Secrecy Act of 1970 (BSA)

The United States was one of the first nations to enact anti-money laundering legislation when it *enacted* the Bank Secrecy Act (BSA) in 1970. The Bank Secrecy Act of 1970 (BSA), also known as the Currency and Foreign Transactions Reporting Act, requires financial institutions in

[5] FATF guidance note on trade-based money laundering

the United States to assist U.S. government agencies in detecting and preventing money laundering. The act specifically requires:

- Financial institutions to keep records of cash purchases of negotiable instruments
- File reports if the daily aggregate exceeds $10,000, and
- Report suspicious activity that may signify money laundering, tax evasion, or other criminal activities.

The BSA was originally passed by the U.S. Congress in 1970[6] and signed by President Richard Nixon into law on October 26, 1970.Until the 1980s, there was a prolonged period of inaction on it, but eventually financial institutions complied with its reporting requirements.

The BSA is sometimes referred to as an anti-money laundering law (AML) or jointly as BSA/AML. An early effort to detect and prevent money laundering, the BSA has since been amended and strengthened by additional anti-money laundering laws. The Financial Crimes Enforcement Network is now the designated administrator of the BSA – with a mission to "safeguard the financial system from the abuses of financial crime, including terrorist financing, money laundering and other illicit activities."

1.3.2 Financial Action Task Force (on Money Laundering)- FATF (1989)

The Financial Action Task Force (on Money Laundering)- FATF, also known by its French name, “Grouped' Action Financière” (GAFI), is an intergovernmental organization founded in 1989 with the initiative of the 1989 G7 Summit in Paris. The mission of FATF is:

- To devise and promote international standards to prevent the growing problem of money laundering;
- Study money laundering trends;
- Monitor legislative, financial and law enforcement activities taken at the national and international level;
- Reporting on compliance, and;
- Issuing recommendations and standards to combat money laundering.

At the time of its formation, FATF had 16 members, which by 2023 had grown to 40[7]. In its first year, FATF issued a report containing forty recommendations to more effectively fight money laundering. These standards were revised in 2023[8] to reflect evolving patterns and techniques in money laundering.

---

[6]https://www.fincen.gov/history-anti-money-laundering-laws

[7] https://www.fatf-gafi.org/en/countries.html

[8] https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Fatf-recommendations.html

Shortly after the 9/11 attacks on the US, FATF expanded its mandate to include AML and combating terrorist financing.

India became a member of FATF in 2010. India is also a member of two FATF Style Regional Bodies (FSRBs)- Asia Pacific Group (APG) and Eurasian Group of Combating Money Laundering and Financing of Terrorism (EAG).[9]

The core work of FATF is to conduct Mutual Evaluation of its Members and to guide and assist SRBs to conduct Mutual evaluation of their respective member jurisdictions.[10]

1.3.3 The International Monetary Fund (IMF)

The International Monetary Fund (IMF) is another important organization. With 189 Member countries, its primary purpose is to ensure stability of the international monetary system. The IMF is concerned about the consequences of money laundering and related crimes affecting the integrity and stability of the financial sector and the broader economy.

The IMF has decades of experience in these areas. It has helped shape policies on anti-money laundering (AML) combatting the financing of terrorism (CFT) and counter-proliferation financing internationally and within its members' national frameworks.

The IMF expanded its AML efforts in 2000 and extended them to CFT after the terrorist attacks on September 11, 2001. In 2004, the IMF Executive Board agreed to make AML/CFT assessments and capacity development a regular part of IMF work.

1.3.4 Bank for International Settlements (BIS) Initiative, (1930)

The Bank for International Settlements (BIS) is an international financial institution which is owned by member banks. Its primary goal is to foster international monetary and financial cooperation while serving as a bank for central banks. With its establishment in 1930, itis the oldest international financial institution. Its initial purpose was to oversee the settlement of World War-I war reparations.

The Bank for International Settlements (BIS) has played a role in anti-money laundering (AML) measures in several ways, including:

- **Providing a forum for cooperation-**The BIS provides a platform for central banks and financial supervisory authorities to exchange information and collaborate.

[9]https://dor.gov.in/fatf and https://www.fatf-gafi.org/en/countries/global-network.html

[10]FATF has been explained in detail in Chapter 8 of this workbook along with the FATF guidance note on Trade-Based Money Laundering.

- **Supporting research and policy analysis-**The BIS conducts research and policy analysis on issues related to monetary and financial stability.
- Acting as a bank for central banks
- The BIS acts as a prime counterparty for central banks in their financial transactions.
- **Issuing guidelines-**The BIS has issued guidelines on sound management of risks related to money laundering.
- **Providing online learning tools-**The BIS offers online learning tools, such as FSI Connect, on AML and CFT in banking.

1.3.5 The Vienna Convention (1988)

Money laundering has been addressed in the UN Vienna 1988 Convention Article 3.1, describing Money Laundering as: *"the conversion or transfer of property, knowing that such property is derived from any offense(s), for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such offense(s) to evade the legal consequences of his actions".*

The Vienna Convention, adopted in December 1988, lays the groundwork for efforts to combat money laundering by creating an obligation for signatory states to criminalize the laundering of money from drug trafficking. It promotes:

- International cooperation in investigations and
- Makes extradition between signatory states applicable to money laundering.

It establishes the principle that domestic bank secrecy provisions should not interfere with international criminal investigations.

1.4. Indian initiatives towards Anti Money Laundering Laws

Anti-money laundering laws in India are a critical aspect of the country's financial and economic framework. They are designed to prevent the illegal flow of funds through the banking and financial system and to promote transparency and accountability in financial transactions. India has implemented a comprehensive set of anti-money laundering laws, which have been updated periodically to keep pace with global best practices. A brief note of these laws is:

1.4.1 Unlawful Activities Prevention Act, 1967 (UAPA)

The Unlawful Activities Prevention Act (UAPA) provides prevention of certain unlawful activities of individuals and associations, and for dealing with terrorist activities, and for matters connected therewith. The act empowers the government to ban organizations involved in terrorist activities and freeze their assets. It also provides for severe punishment for those involved in such activities.

Section 35 of Unlawful Activities (Prevention) Act 1967

Under Section 35 of the Act, the Central government may, by notification, in the Official Gazette, —

(a) add an organisation to the First Schedule
(b) add also an organisation to the First Schedule, which is identified as a terrorist organisation in a resolution adopted by the Security Council under Chapter VII of the Charter of the United Nations, to combat international terrorism;
(c) remove an organisation from the First Schedule;
(d) amend the First Schedule in some other way.

The central government exercises its power in respect of an organisation only if it believes that it is involved in terrorism and the central government may, by notification in the Official Gazette, add to or remove or amend the Second Schedule or Third Schedule.

Section 51A of Unlawful Activities (Prevention) Act 1967

Under Section 51A of Unlawful Activities (Prevention) Act 1967[11] and orders issued thereunder, the Central Government has power to:

- freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism;
- prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism;
- prevent the entry into or the transit through India of individuals listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

1.4.2 Foreign Exchange Management Act, 1999 (FEMA)

This Act consolidates and amends the laws relating to foreign exchange with the objective of facilitating external trade and payments and for promoting the orderly development and maintenance of foreign exchange market in India. The act regulates foreign exchange

[11] Source- https://www.indiacode.nic.in/bitstream/123456789/1470/1/a1967-37.pdf

transactions and prohibits money laundering and financing of terrorism through such transactions.

1.4.3 Prevention of Money Laundering Act, 2002 (PMLA)

In India, Prevention of Money Laundering Act, 2002 (PMLA) was enacted to fight against the criminal offence of legalizing the income/profits from an illegal source. The act provides for the prevention, detection, and prosecution of money laundering activities. It requires financial institutions to maintain records of all transactions and report any suspicious activity to the authorities. The Prevention of Money Laundering Act, 2002 enables the government or the public authority to confiscate the property earned from the illegally gained proceeds. This Act, has been dealt in detail in the next chapter.

1.4.4 Financial Intelligence Unit (FIU), FINGATE Registration, Role of Designated Director and Principal Officer

Financial Intelligence Unit – India (FIU-IND) was set by the Government of India vide O.M. dated 18th November 2004 as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspected financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and financing of terrorism. FIU-IND is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the finance minister.

The main functions of FIU-IND are to receive cash/suspicious transaction reports, analyse them and, as appropriate, disseminate valuable financial information to intelligence/enforcement agencies and regulatory authorities. The functions of FIU-IND are:

- **Collection of Information**: Act as the central reception point for receiving Cash Transaction reports (CTRs), Non-Profit Organisation Transaction Report (NTRs), Cross Border Wire Transfer Reports (CBWTRs), Reports on Purchase or Sale of Immovable Property (IPRs) and Suspicious Transaction Reports (STRs) from various reporting entities.
- **Analysis of Information**: Analyze received information in order to uncover patterns of transactions suggesting suspicion of money laundering and related crimes.
- **Sharing of Information**: Share information with national intelligence/law enforcement agencies, national regulatory authorities and foreign Financial Intelligence Units.
- **Act as Central Repository:** Establish and maintain national data base on the basis of reports received from reporting entities.
- **Coordination**: Coordinate and strengthen collection and sharing of financial intelligence through an effective national, regional and global network to combat money laundering and related crimes.

- **Research and Analysis**: Monitor and identify strategic key areas on money laundering trends, typologies and developments.

1.4.5 FINGate Registration

All regulated entities licensed with IFSCA are mandatorily required to register with the Financial Intelligence Unit of India (FIU-IND) by completing the enrolment on the FINGate 2.0 Portal.[12]

The registration process involves furnishing the details about the business, the Principal Officer, and the regulated entity's Designated Director, who shall take care of the AML program within the organisation. Non-registration with FIU-IND is treated as non-compliance with the IFSCA (AML, CFT, and KYC) Guidelines.

Registration on FIU-IND FINGate 2.O portal is a two-step procedure. The first step is Regulated Entity registration, and second step is Designated Director and Principal Officer registration.

1.4.6 AML & CFT Guidelines

The AML & CFT guidelines have been envisaged in the Prevention of Money Laundering Act, 2002 (PMLA). These guidelines specify record keeping and reporting obligations for Financial Institutions and persons carrying on designated business or profession. The PMLA 2002 has been dealt in detail in Chapter 2.

Persons carrying on designated business or profession are defined in Clause (s) of sub-section (1) of Section 2 of the PMLA (covered in chapter 2). Sub-clause (vi) of the said clause includes within the ambit of 'person carrying on designated business or profession' such persons who carry on activities as the Central Government may, by notification, designate from time-to-time.

Further, the AML & CFT Guidelines for reporting entities including related to Virtual Digital Assets (VDA) aim to provide a summary of the provisions of the applicable anti money laundering, counter-terrorism financing and proliferation financing legislations in India. They are:

- The Prevention of Money Laundering Act, 2002 (hereinafter referred to as the "PMLA"),
- The Unlawful Activities (Prevention) Act, 1967 (hereinafter referred to as the "UAPA"),
  The Weapons of Mass Destruction and Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (hereinafter referred to as the "WMDA") and rules there under.

[12] FINGate 2.0 is the primary platform through which data associated with money laundering or other crimes is furnished to FIU-IND. FINGate 2.0 is FINNET 2.0's front-end web portal used by regulated entities to report suspicious financial transactions.

Further, IFSCA has introduced IFSCA (AML, CFT and KYC) Guidelines for the regulated entities of IFSC ecosystem, which has been discussed in detail in Chapter No. 5.

1.4.7 The Weapons of Mass Destruction and Delivery Systems (Prohibition of Unlawful Activities) Act, 2005

Under Section 12 of The Weapons of Mass Destruction and Delivery Systems (Prohibition of Unlawful Activities) Act, 2005, no person who is a resident in India shall, for a consideration under the terms of an actual or implied contract, knowingly facilitate the execution of any transaction which is prohibited or regulated under this Act:

Provided that a mere carriage, without knowledge, of persons, goods or technology, or provision of services, including by a public or private carrier of goods, courier, tele-communication, postal service provider or financial service provider, shall not be an offence for the purposes of this section.

1.4.8 International Financial Services Centre (IFSC)

Financial centres that cater to customers outside their own jurisdiction are referred to as International Financial Centres (IFCs) or Offshore Financial Centers (OFCs). All these centres are 'international' in the sense that they deal with the flow of finance and financial products/services across borders.

The Gujarat International Finance Tec-City (GIFT City) International Financial Services Centre (GIFT IFSC) is a financial centre and special economic zone in GIFT City of India. It was established in 2015 as a financial hub to provide world-class infrastructure and services for financial institutions and companies operating in areas such as banking, insurance, capital markets, and asset management. GIFT IFSC is regulated by the International Financial Services Centres Authority (IFSCA), an independent regulator exclusive to the zone.

The Government of India established International Financial Services Centres Authority in April 2020 under the International Financial Services Centres Authority Act passed by the Indian Parliament. For the first time, the regulatory powers of four financial services regulators in India, namely, Reserve Bank of India (RBI), Securities & Exchange Board of India (SEBI), Insurance Regulatory Development Authority of India (IRDAI), Pension Fund Regulatory Development Authority of India (PFRDAI), have been vested in IFSCA.

The IFSCA is a unified authority for development and regulation of financial products, financial services and financial institutions in the International Financial Services Centre in India in the areas of banking, insurance, securities and funds management. The IFSCA is committed to provide a comprehensive and consistent regulatory framework based on global best practices with a special focus on ease of doing business.

As a unified regulator IFSCA is committed to ensuring financial stability and protection of the interests of investors. At the same time, it allows enough space for financial innovations with adequate risk management measures in place. The IFSCA is also committed to ensure that regulatory environment is fully FATF compliant with strong enforcement measures of AML and CFT in place. Following the PMLA and the overall FATF Recommendations, IFSCA has issued the IFSCA (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022.

The prevention of money laundering is essential to combat financial terrorism effectively. The implementation of robust regulations and guidelines, improved collaboration between financial institutions and governments, and the use of technology-driven solutions are considered crucial to prevent the financing of terrorism. Collective action approach of the institutions aims to combat financial terrorism and ensure global financial stability and security.

Sample Questions

1. Criminals practice money laundering by which of the following ways?
   a) Disguising the source of ill-gotten gains
   b) Changing the form of criminal proceeds
   c) Elsewhere moving profits of criminal acts
   d) All of the above

2. Why are Anti Money Laundering Laws very important for a country?
   a) They help in preventing criminals from hiding illegally obtained money.
   b) They let criminals enjoy the ill-gotten profits.
   c) They have minimum social consequences.
   d) They erode the integrity of a nation's Financial Institutions.

3. What is the stage of money laundering, when the illegally obtained funds are introduced in the financial system, known as?
   a) Extraction
   b) Placement
   c) Layering
   d) Integration

4. The main function of which organisation is to receive cash/suspicious transaction reports, analyse them and, disseminate valuable financial information to intelligence/enforcement agencies and regulatory authorities.?
   a) RBI
   b) SEBI
   c) FIU-IND
   d) IRDAI

5. It is mandatory for all regulated entities licensed with IFSCA to register with the Financial Intelligence Unit of India (FIU-IND) by completing the enrolment which Portal?
   a) FINGate 2.0 Portal
   b) SEBI Portal
   c) FIU-IND Portal
   d) RBI Portal

Chapter-2 Prevention of Money Laundering Act, 2002

Learning Objective - After studying this chapter, you should know about:

- Definition, objective and explanation of the concept and importance of Prevention of Money Laundering as per PMLA 2002.

Authorities entrusted for investigations regarding money la

2.1 Prevention of Money Laundering Act, 2002 (PMLA)

Prevention of Money Laundering Act (PMLA) forms the core of the legal framework put in place by India to combat money laundering. It is an act to prevent money-laundering and to provide for confiscation of property derived from, or involved in, money-laundering and for matters connected therewith or incidental thereto. Prevention of Money Laundering Act (PMLA) and the Prevention of Money Laundering Rules (PMLR) notified there under came into force with effect from July 1, 2005.

Director, FIU-IND and Director (Enforcement) have been conferred with exclusive and concurrent powers under relevant sections of the Act to implement the provisions of the Act. The PMLA and rules notified thereunder impose obligation on banking companies, financial institutions, and intermediaries and persons carrying on a designated business or profession, to verify identity of clients, maintain records and furnish information to FIU-IND.

2.1.1 Section 2 of the PMLA 2002

This section defines terms used in the Act

(1) In this Act, unless the context otherwise requires, —

(a) "Adjudicating Authority" means an Adjudicating Authority appointed under sub-section (1) of section 6;

(b) "Appellate Tribunal" means the Appellate Tribunal established under section 25;

(c) "Assistant Director" means an Assistant Director appointed under sub-section (1) of section 49;

(d) "attachment" means prohibition of transfer, conversion, disposition or movement of property by an order issued under Chapter III;

(da) "authorised person" means an authorised person as defined in clause (c) of section 2 of the Foreign Exchange Management Act, 1999(42 of 1999);

(e) "banking company" means a banking company or a co-operative bank to which the Banking Regulation Act, 1949 (10 of 1949) applies and includes any bank or banking institution referred to in section 51 of that Act;

(f) "Bench" means a Bench of the Appellate Tribunal;

(fa) "beneficial owner" means an individual who ultimately owns or controls a client of a reporting entity or the person on whose behalf a transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person[13];

(g) "Chairperson" means the Chairperson of the Appellate Tribunal;

(h) "chit fund company" means a company managing, conducting or supervising, as foreman, agent or in any other capacity, chits as defined in section 2 of the Chit Funds Act, 1982 (40 of 1982);

(ha) "client" means a person who is engaged in a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who engaged in the transaction or activity, is acting;

(i) "co-operative bank" shall have the same meaning as assigned to it in clause (dd) of section 2 of the Deposit Insurance and Credit Guarantee Corporation Act, 1961 (47 of 1961);

(ia) "corresponding law" means any law of any foreign country corresponding to any of the provisions of this Act or dealing with offences in that country corresponding to any of the scheduled offences;

(ib) "dealer" has the same meaning as assigned to it in clause (b) of section 2 of the Central Sales Tax Act, 1956 (74 of 1956);

(j) "Deputy Director" means a Deputy Director appointed under sub-section (1) of section 49;

(k) "Director" or "Additional Director" or "Joint Director" means a Director or Additional Director or Joint Director, as the case may be, appointed under sub-section (1) of section 49;

(l) "financial institution" means a financial institution as defined in clause (c) of section 45-I of the Reserve Bank of India Act, 1934 (2 of 1934) and includes a chit fund company, a housing finance institution, an authorised person, a payment system operator, a nonbanking financial company and the Department of Posts in the Government of India;

---

[13]From the IFSCA perspective the meaning of beneficial owner has been explained in point 6.3.6 of this book.

(m) “housing finance institution” shall have the meaning as assigned to it in clause (d) of section 2 of the National Housing Bank Act, 1987 (53 of 1987);

(n) “intermediary” means, —

(i) a stock-broker, sub-broker share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser or any other intermediary associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992 (15 of 1992); or

(ii) an association recognised or registered under the Forward Contracts (Regulation) Act, 1952 (74 of 1952) or any member of such association; or

(iii) intermediary registered by the Pension Fund Regulatory and Development Authority; or

(iv) a recognised stock exchange referred to in clause (f) of section 2 of the Securities Contracts (Regulation) Act, 1956 (42 of 1956);

(na) “investigation” includes all the proceedings under this Act conducted by the Director or by an authority authorised by the Central Government under this Act for the collection of evidence;

(o) “Member” means a Member of the Appellate Tribunal and includes the Chairperson;

(p) “money-laundering” has the meaning assigned to it in section 3;

(q) “non-banking financial company” shall have the same meaning as assigned to it in clause (f) of section 45-I of the Reserve Bank of India Act, 1934 (2 of 1934);

(r) “notification” means a notification published in the Official Gazette;

(ra) “offence of cross border implications”, means—

(i) any conduct by a person at a place outside India which constitutes an offence at that place and which would have constituted an offence specified in Part A, Part B or Part C of the Schedule, had it been committed in India and if such person the proceeds of such conduct or part thereof to India; or

(ii) any offence specified in Part A, Part B or Part C of the Schedule which has been committed in India and the proceeds of crime, or part thereof have been transferred to a place outside India or any attempt has been made to transfer the proceeds of crime, or part thereof from India to a place outside India. Explanation.—Nothing contained in this clause shall adversely affect any investigation, enquiry, trial or proceeding before any authority in respect of the offences specified in Part A or Part B of the Schedule to the Act before the commencement of the Prevention of Money-laundering (Amendment) Act, 2008

(rb) “payment system” means a system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them.
Explanation. —For the purposes of this clause, “payment system” includes the systems enabling credit card operations, debit card operations, smart card operations, money transfer operations or similar operations;

(rc) “payment system operator” means a person who operates a payment system and such person includes his overseas principal.
Explanation. —For the purposes of this clause, “overseas principal” means, —

(i) in the case of a person, being an individual, such individual residing outside India, who owns or controls or manages, directly or indirectly, the activities or functions of payment system in India;
(ii) in the case of a Hindu undivided family, Karta of such Hindu undivided family residing outside India who owns or controls or manages, directly or indirectly, the activities or functions of payment system in India;
(iii) in the case of a company, a firm, an association of persons, a body of individuals, an artificial juridical person, whether incorporated or not, such company, firm, association of persons, body of individuals, artificial juridical person incorporated or registered outside India or existing as such and which owns or controls or manages, directly or indirectly, the activities or functions of payment system in India;

(s) “person” includes; —
(i) an individual,
(ii) a Hindu undivided family,
(iii) a company,
(iv) a firm,
(v) an association of persons or a body of individuals, whether incorporated or not,
(vi) every artificial juridical person, not falling within any of the preceding sub-clauses, and
(vii) any agency, office or branch owned or controlled by any of the above persons mentioned in the preceding sub-clauses;

(sa) “person carrying on designated business or profession” means, —

- a person carrying on activities for playing games of chance for cash or kind, and includes such activities associated with casino;
- Inspector-General of Registration appointed under section 3 of the Registration Act, 1908 as may be notified by the Central Government;
- real estate agent, as may be notified by the Central Government;

- dealer in precious metals, precious stones and other high value goods, as may be notified by the Central Government;
- person engaged in safekeeping and administration of cash and liquid securities on behalf of other persons, as may be notified by the Central Government; or
- person carrying on such other activities as the Central Government may, by notification, so designate, from time-to time;

(sb) "precious metal" means gold, silver, platinum, palladium or rhodium or such other metal as may be notified by the Central Government;

(sc) "precious stone" means diamond, emerald, ruby, sapphire or any such other stone as may be notified by the Central Government;

(t) "prescribed" means prescribed by rules made under this Act;

(u) "proceeds of crime" means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property or where such property is taken or held outside the country, then the property equivalent in value held within the country or abroad; Explanation.—For the removal of doubts, it is hereby clarified that "proceeds of crime" include property not only derived or obtained from the scheduled offence but also any property which may directly or indirectly be derived or obtained as a result of any criminal activity relatable to the scheduled offence.

(v) "property" means any property or assets of every description, whether corporeal or incorporeal, movable or immovable, tangible or intangible and includes deeds and instruments evidencing title to, or interest in, such property or assets, wherever located; Explanation. —For the removal of doubts, it is hereby clarified that the term "property" includes property of any kind used in the commission of an offence under this Act or any of the scheduled offences;

(va) "real estate agent" means a real estate agent as defined in clause (88) of section 65 of the Finance Act, 1994;

(w) "records" include the records maintained in the form of books or stored in a computer or such other form as may be prescribed;

(wa) "reporting entity" means a banking company, financial institution, intermediary or a person carrying on a designated business or profession;

(x) "Schedule" means the Schedule to this Act;

(y) “scheduled offence” means—

(i) the offences specified under Part A of the Schedule; or
(ii) the offences specified under Part B of the Schedule if the total value involved in such offences is one crore rupees or more; or
(iii) the offences specified under Part C of the Schedule;

(z) “Special Court” means a Court of Session designated as Special Court under sub-section (1) of section 43;

(za) “transfer” includes sale, purchase, mortgage, pledge, gift, loan or any other form of transfer of right, title, possession or lien;

(zb) “value” means the fair market value of any property on the date of its acquisition by any person, or if such date cannot be determined, the date on which such property is possessed by such person.

(2) Any reference, in this Act or the Schedule, to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provisions of the corresponding law, if any, in force in that area.

2.1.2 Section 3 of the PMLA 2002

This section gives the definition of Offence of Money Laundering. Whosoever, directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of offence of money-laundering. Further, the Act clarifies that a person shall be guilty of offence of money-laundering if such person is found to have directly or indirectly attempted to indulge or knowingly assisted or knowingly is a party or is actually involved in one or more of the following processes or activities connected with proceeds of crime, namely: —

(a) concealment; or
(b) possession; or
(c) acquisition; or
(d) use; or
(e) projecting as untainted property; or
(f) claiming as untainted property, in any manner whatsoever

The process or activity connected with proceeds of crime is a continuing activity and continues till such time a person is directly or indirectly enjoying the proceeds of crime by its concealment or possession or acquisition or use or projecting it as untainted property or claiming it as untainted property in any manner whatsoever.

The PMLA is divided in multiple sections. An illustrative list regarding applicability/scope of coverage of these sections[14] is as mentioned below:

Sections	**Scope of Coverage**
Section 1	Short title, extent & Commencement
Section 2	Definitions
Section 3	Offence of Money Laundering
Section 4	Punishment for Money Laundering
Section 5	Attachment of property involved in money-laundering.
Section 11A	Verification of identity by reporting entity
Section 12	Reporting entity to maintain records
Section 12A & 12 AA	Access to Information
Section 13	Powers of the Director
Section 14	No civil or criminal proceedings against reporting entity, its Directors & Employees in certain cases
Section 15	Procedure and manner of furnishing information by reporting entities
Section 26	Appeals to Appellate Tribunal
Section 39	Right of appellant to take assistance of authorised representative and of Government to appoint presenting officers
Section 40	Members etc. to be public servants
Section 41	Civil court not to have jurisdiction
Section 42	Appeal to high court
Section 44	Offences triable by special courts
Section 48	Authorities under the Act
Section 49	Appointment and powers of authorities and other officers
Section 50	Powers of authorities regarding summons, production of documents and to give evidence etc.
Section 54	Certain officers and others to assist in inquiry etc.
Section 56	Agreements with foreign countries
Section 66	Disclosure of information
Section 69	Recovery of Fine or Penalty
Section 73	Power to make Rules
Section 75	Power to remove difficulties

[14]Source: https://fiuindia.gov.in/files/AML_Legislation/pmla_2002.html

2.1.3 Section 4 of the PMLA 2002

As per **Section 4 of the PMLA 2002**, "Whoever commits the offence of money-laundering is punishable with rigorous imprisonment for a term which will not be less than three years but which may extend to seven years and shall also be liable to fine.
However, it may be noted that where the proceeds of crime involved in money-laundering relates to any offence specified under paragraph 2 of Part A of the Schedule, the provisions of this section shall have effect as if for the words “which may extend to seven years”, the words “which may extend to ten years” had been substituted.

2.1.4 Section 5 of the PMLA 2002

As prescribed under **Section 5 of the Act**, where the Director or any other officer not below the rank of Deputy Director authorised by the Director for the purposes of this section, has reason to believe (recorded in writing), on the basis of material in his possession, that--

(a) any person is in possession of any proceeds of crime; and

(b) such proceeds of crime are likely to be concealed, transferred or dealt with in any manner which may result in frustrating any proceedings relating to confiscation of such proceeds of crime may, by order in writing, provisionally attach such property for a period not exceeding one hundred and eighty days from the date of the order, in such manner as may be prescribed

2.1.5 Section 12 of the PMLA 2002

As per Section 12 of the PMLA 2002, the requirement for maintenance of records by reporting entities has been specified. According to the section

(1) Every reporting entity is required to—
   - (a) maintain a record of all transactions, in such manner as to enable it to reconstruct individual transactions;
   - (b) furnish to the Director within such time as may be prescribed, information relating to such transactions, whether attempted or executed, the nature and value of which may be prescribed;
   - (c) maintain record of documents evidencing identity of its clients and beneficial owners as well as account files and business correspondence relating to its clients.

(2) Every information maintained, furnished or verified, save as otherwise provided under any law for the time being in force, shall be kept confidential.

(3) The records referred to in clause (a) of sub-section (1) shall be maintained for a period of five years from the date of transaction between a client and the reporting entity.

(4) The records referred to in clause (c) of sub-section (1) shall be maintained for a period of five years after the business relationship between a client and the reporting entity has ended or the account has been closed, whichever is later.

(5) The Central Government may, by notification, exempt any reporting entity or class of reporting entities from any obligation under this Chapter.

2.1.6 Section 56 of the PMLA 2002

As illustrated under **Section 56 of the PMLA 2002** the international co-operation between countries for the purpose of prevention of money laundering has been specified. Accordingly

(1) The Central Government may enter into an agreement with the Government of any country outside India for:

(a) enforcing the provisions of this Act;
(b) exchange of information for the prevention of any offence under this Act or under the corresponding law in force in that country or investigation of cases relating to any offence under this Act, and may, by notification in the Official Gazette, make such provisions as may be necessary for implementing the agreement.

(2) The Central Government may, by notification in the Official Gazette, direct that the application of this Chapter in relation to a contracting State with which reciprocal arrangements have been made, shall be subject to such conditions, exceptions or qualifications as are specified in the said notification.

2.2 Maintenance of records and furnishing of reports to FIU-IND[15]

For effective implementation of the Act, maintenance and reporting of records is an important requirement. Under the PML Rules, Rule 3 – Maintenance of records of transactions, the following transactions have been specified, for which records have to be maintained and reports are to be furnished to FIU-IND[16]:

(a) All cash transactions of the value of more than rupees 10 lakh or its equivalent in foreign currency.

[15] Note: No cash transactions are permitted in IFSC domain.
[16] Source: https://fiuindia.gov.in/files/AML_Legislation/notification.htmland https://fiuindia.gov.in/pdfs/downloads/Brochures%20on%20FIU.pdf

(b) All series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency;
(c) All transactions involving receipts by non - profit organisations of value more than rupees ten lakh, or its equivalent in foreign currency;
(d) All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;
(e) All suspicious transactions, whether or not made in cash, including attempted transactions.
(f) All cross-border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India;
(g) All purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity.

The Suspicious Transaction Report mentioned at para (e) above should be furnished within seven working days on being satisfied that the transaction is suspicious.

The information in respect of immoveable property transactions referred to in (g) above should be furnished to FIU-IND every quarter by the 15th day of the month succeeding the quarter.

All other reports need to be furnished on a monthly basis by the 15th day of the succeeding month.

Further, every reporting entity is necessarily required to furnish information to Director, FIU-IND online in a standard format prescribed for the purpose. For this purpose, the reporting entity has to register itself with FIU-IND.

2.2.1 Suspicious Transaction

Suspicious Transaction means a transaction (including an attempted transaction) whether or not made in cash which, to a person acting in good faith:

a) gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
b) appears to be made in circumstances of unusual or unjustified complexity; or
c) appears to have no economic rationale or bona fide purpose; or
d) gives rise to a reasonable ground of suspicion that it may involve financing of activities relating to terrorism.
Designation of officers for ensuring compliance with provisions of PMLA.

Each reporting entity has to appoint certain designated officials to implement the provisions of the Act in the reporting Organisation.

2.2.2 Appointment of a Principal Officer

The Principal Officer is an officer designated by a registered intermediary who should be an officer at the management level. Principal Officer is designated by a reporting entity for the purpose of Section 12 of PMLA. Rule 7 of the PML Rules requires every reporting entity to communicate the name, designation and address of the Principal Officer to the Director, FIU-IND. The Principal Officer would act as a central reference point in facilitating onward reporting of suspicious transactions.

2.2.3 Appointment of a Designated Director

In addition to the existing requirement of designation of a Principal Officer, the registered intermediaries shall also designate a person as a 'Designated Director'. Designated director is a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the PMLA Act and the Rules and includes:

(i) the Managing Director or a whole-time Director if the reporting entity is a company,
(ii) the managing partner if the reporting entity is a partnership firm,
(iii) the proprietor if the reporting entity is a proprietorship concern[17]
(iv) the managing trustee if the reporting entity is a trust,
(v) a person or individual who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a body of individuals, and
(vi) a person who is heading the reporting entity in India, if the reporting entity is located in an International Financial Services Centre; and
(vii) such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above.

Explanation. —For the purpose of this clause, the terms “Managing Director” and “Whole-time Director” shall have the meaning assigned to them in the Companies Act, 2013 (18 of 2013);

2.2.4 Compliance Requirements for IFSCA Regulated Entities

The International Financial Services Centres Authority (IFSCA) requires entities operating in an IFSC to comply with specific provisions under the Prevention of Money Laundering Act (PMLA), 2002. The IFSCA (Anti Money Laundering, Counter-Terrorist Financing, and Know Your

[17]In IFSCA the permitted legal forms are company/partnership firms/body corporates; proprietory concerns are not allowed.

Customer) Guidelines, 2022, lay out compliance expectations, including mandated exemptions and operational safeguards.

Key Requirements for IFSC Entities

(i) Business Risk Assessment: All financial institutions (including exempted ones) must conduct and document a Business Risk Assessment (BRA).
(ii) Transaction Monitoring: All monetary receipts must only be through accounts maintained with a banking unit in the IFSC.
(iii) KYC & Due Diligence: Entities must follow robust KYC (Know Your Customer) procedures, including enhanced diligence for high-risk clients, identification of beneficial owners, source of funds, and ongoing monitoring.
(iv) Reporting Obligations: Suspicious transactions and specific high-value transactions must be reported to relevant authorities, in line with the PMLA and IFSCA guidelines.

Exemptions and continued obligations

(i) Certain entities, such as international branch campuses of foreign universities and service providers within the same financial group (not in FATF high-risk jurisdictions), are exempt from direct AML/CTF/KYC compliance but must still do a business risk assessment. If any AML/CTF risks are identified, normal compliance obligations under the PMLA and the IFSCA Guidelines resume.

Exempted institutions are not relieved from all oversight and are still required to conduct formal risk assessment and maintain relevant records and safeguards.[18]

2.3 Main Authorities entrusted for investigations[19]

2.3.1 Directorate of Enforcement

The Directorate of Enforcement is a multi-disciplinary organization mandated with investigation of offence of money laundering and violations of foreign exchange laws. The statutory functions of the Directorate include enforcement of following Acts:

- The Prevention of Money Laundering Act, 2002 (PMLA):

[18]IFSCA has exempted certain entities and activities from the applicability of the IFSCA AML, CFT and KYC Guidelines, as per its circular dated 18/11/2024: https://ifsca.gov.in/CommonDirect/GetFileView?id=d09c93fc98191af1801a5914f316fdf7&fileName=18-11-2024-circular-exempting-certain-entitiesactivities-from-the-applicability-of-the-guidelines18112024114602.pdf&TitleName=Legal

[19] Source: https://enforcementdirectorate.gov.in/what-we-do

- The Foreign Exchange Management Act, 1999 (FEMA)
- The Fugitive Economic Offenders Act, 2018 (FEOA)
- Sponsoring agency under COFEPOSA

2.3.2 Financial Intelligence Unit – India (FIU-IND)

FIU-IND was set by the Government of India vide O.M. dated 18th November 2004 as the central national agency responsible for receiving, processing, analysing and disseminating information relating to suspect financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and financing of terrorism. FIU-IND is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

2.3.3 Adjudicating Authority

Section 6 of the PMLA, 2002 defines Adjudicating authority. It is constituted by the Central Government, and it exercises quasi-judicial powers, such as issuing notices, adjudicating property attachments, and confirming confiscations.[20]

2.3.4 Other Regulatory Agencies

Depending on the scheduled offence, agencies like IFSCA, SEBI, CBI, customs, and police may be involved for parallel investigation of predicate (scheduled) offences.

[20]Source: https://enforcementdirectorate.gov.in/sites/default/files/Act%26rules/THE%20PREVENTION%20OF%20MONEY%20LAUNDERING%20ACT%2C%202002.pdf

Sample Questions

1. Under the Prevention of Money Laundering Act (PMLA), which authorities have been conferred with exclusive and concurrent powers to implement the provisions of the Act?
   a) Chairperson, Central Board of Direct Taxes (CBDT)
   b) Director, FIU-IND and Director (Enforcement)
   c) Secretary, Department of Revenue
   d) Comptroller & Auditor General

2. As per Section 4 of the PMLA 2002, whoever commits the offence of money-laundering shall be punishable with rigorous imprisonment for a term which shall fall in between
   a) 3-4 years
   b) 4-5 years
   c) 3-7 years
   d) None of the above

3. Which of the following categories of persons are designated as reporting entities under the PMLA and PML Rules?
   a) Only stock exchanges and depositories
   b) Banking companies, financial institutions, intermediaries, and persons carrying on designated businesses
   c) Only insurers and pension fund regulators
   d) Government departments and public sector undertakings only

4. Key Requirements for IFSC Entities under the IFSCA (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines 2022 and PMLA 2002 are:
   a) Business Risk Assessment
   b) Transaction Routing
   c) KYC & Due Diligence
   d) All of the above

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

Learning Objective - After studying this chapter, you should know about:

- Definition, objective and process of implementation of PML (Maintenance of Records) Rules, 2005
- Detailed explanation of verifying the identity of the client/ true beneficial owner of the assets under Client Due Diligence rules under PMLR, 2005.

3.1 Introduction to the Prevention of Money-laundering (Maintenance of Records) Rules, 2005

An act is a law or the statute which has been passed by the legislature and approved by the President of India. Rules, on the other hand, help in governing laws. Rules are created after an act to define how the act will be implemented and performed. Rules are secondary to the act, and are created to provide flexibility in implementation.

In exercise of the powers conferred by section 73 of the Prevention of Money-Laundering Act, 2002 (15 of 2003), the Central Government in consultation with the Reserve Bank of India, hereby made the following rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of records of the identity of the clients of the banking companies, financial institutions and intermediaries. Further, vide Gazette Notification dated 7th March, 2023, the above mentioned rules were amended and to be called as the Prevention of Money-laundering (Maintenance of Records) Amendment Rules, 2023.

The rules require entities to:

- Develop internal controls: Create policies, procedures, systems, and controls to prevent financial crimes
- Conduct customer due diligence: Follow a process before onboarding customers or executing transactions
- Report suspicious activity: Report suspicious transactions and other specified activities
- Maintain client identity records: a reporting entity shall keep records of the client identity in the manner as may be specified by the regulator from time to time.

Thus, we may understand that by mandating robust customer verification, due diligence and reporting practices, IFSCA, SEBI and RBI aim to create a secure environment within the financial sector to prevent illicit financial activities.

3.2 Maintenance of Records of Transactions

3.2.1 Maintenance of Records of Transactions (Nature and Value) (Rule 3)

Rule 3 of PMLR, 2005 is important because it outlines the responsibilities of reporting entities, their officers, and employees in maintaining information. The rule states:

Every reporting entity shall maintain the record of all transactions including, the record of -

(A) all cash transactions of the value of more than ten lakh rupees or its equivalent in foreign currency;

(B) all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency;

(BA) all transactions involving receipts by non-profit organisations of value more than rupees ten lakh, or its equivalent in foreign currency;

(C) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;

(D) all suspicious transactions whether or not made in cash and by way of -

- (i) deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of:
  - a) cheques including third party cheques, pay orders, demand drafts, cashiers cheques or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits, or
  - b) travelers cheques,
  - c) transfer from one account within the same banking company, financial institution and intermediary, as the case may be, including from or to Nostro and Vostro accounts, or
  - d) any other mode in whatsoever name it is referred to;

- (ii) credits or debits into or from any non-monetary accounts such as d-mat account, security account in any currency maintained by the banking company, financial institution and intermediary, as the case may be;

(iii) money transfer or remittances in favour of own clients or non-clients from India or abroad and to third party beneficiaries in India or abroad including transactions on its own account in any currency by payment orders, cashiers, cheques, demand drafts, telegraphic or wire transfers, electronic remittances or transfers, internet transfers, Automated Clearing House remittances, lock box driven transfers or remittances, remittances for credit or loading to electronic cards or any other mode of money transfer by whatsoever name it is called;

(iv) loans and advances including credit or loan substitutes, investments and contingent liability by way of –

a) subscription to debt instruments such as commercial paper, certificate of deposits, preferential shares, debentures, securitised participation, interbank participation or any other investments in securities or the like in whatever form and name it is referred to, or
b) purchase and negotiation of bills, cheques and other instruments, or
c) foreign exchange contracts, currency, interest rate and commodity and any other derivative instrument in whatsoever name it is called, or
d) letters of credit, standby letters of credit, guarantees, comfort letters, solvency certificates and any other instrument for settlement and/or credit support;

(v) collection services in any currency by way of collection of bills, cheques, instruments or any other mode of collection in whatsoever name it is referred to.

(E) all cross-border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India.

(F) all purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be.

<u>Rule 3A Implementation of policies by groups:</u>

As per Rule 3A,

(1) Every reporting entity, which is part of a group, shall implement group-wide programmes against money laundering and terror financing, including group-wide policies for sharing information required for the purposes of client due diligence and money laundering and terror finance risk management and such programmes shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

(2) Groups are required to implement group-wide policies for the purpose of discharging obligations under the provisions of Chapter IV the Prevention of Money Laundering Act, 2002.

3.2.2 Records Containing Information (Rule 4)

The records referred to in rule 3 shall contain all necessary information specified by the regulator to permit reconstruction of individual transaction including the following information:

(a) the nature of the transactions
(b) the amount of the transaction and the currency in which it was denominated
(c) the date on which the transaction was conducted; and
(d) the parties to the transaction.

3.2.3 Procedure and Manner of Maintaining Information (Rule 5)

(1) Every reporting entity shall maintain information in respect of transactions with its client referred to in rule 3 in accordance with the procedure and manner as may be specified by its regulator from time to time.
(2) Every reporting entity shall evolve an internal mechanism for maintaining such information in such form and manner and at such intervals as may be specified by its regulator from time to time.
(3) It shall be the duty of every reporting entity, its designated director, officers and employees to observe the procedure and the manner of maintaining information as specified by its regulator under sub-rule (1).

3.2.4 Procedure and manner of furnishing information (Rule 7)

(1) Every reporting entity shall communicate to the Director the name, designation and address of the Designated Director and the Principal Officer.
(2) The Principal Officer shall furnish the information referred to in clauses (A), (B), (BA), (C), (D), (E) and (F) of sub-rule (1) of rule 3 to the Director on the basis of information available with the reporting entity. A copy of such information shall be retained by the Principal Officer for the purposes of official record.
(3) Every reporting entity shall evolve an internal mechanism having regard to any guidelines issued by the Director in consultation with, its regulator, for detecting the transactions referred to in clauses (A), (B), (BA), (C), (D), (E) and (F) of sub-rule (1) of rule 3 and for furnishing information about such transactions in such form as may be directed by the Director in consultation with, its Regulator.

(4) It shall be the duty of every reporting entity, its designated director, officers and employees to observe the procedure and the manner of furnishing information as specified by the Director in consultation with, its Regulator.

3.2.5 Furnishing of information to the Director (Rule 8)

(1) The Principal Officer of a reporting entity shall furnish the information in respect of transactions referred to in clauses (A), (B), (BA), (C) and (E) of sub-rule (1) of rule 3 every month to the Director by the 15th day of the succeeding month.

(2) The Principal Officer of a reporting entity shall furnish the information promptly in writing or by fax or by electronic mail to the Director in respect of transactions referred to in clause (D) of sub-rule (1) of rule 3 not later than seven working days on being satisfied that the transaction is suspicious.

(3) The Principal Officer of a reporting entity shall furnish, the information in respect of transactions referred to in clause (F) of sub-rule (1) of rule 3, every quarter to the Director by the 15th day of the month succeeding the quarter.

(4) For the purpose of this rule, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-reported transaction beyond the time limit as specified in this rule shall constitute a separate violation.

(5) Notwithstanding anything contained in sub-rule (1) and (3) the Reporting Officer shall furnish the information in respect of transactions referred to in clauses (A), (B), (BA), (C) and (E) of sub rule (1) of rule 3 for the months of March 2020, April 2020 and May 2020, and in respect of transactions referred to in clauses (F) of sub rule (1) of rule 3 for the quarter January-March 2020) by the 30th June, 2020.

(6) Every reporting entity, its Directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 and furnishing of information to the Director is kept confidential.

Provided that nothing in this rule shall inhibit sharing of information under rule 3A of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

3.2.6 Client Due Diligence (Rule 9)

(1) Every reporting entity shall at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations:

(a) identify its clients, verify their identity using reliable and independent sources of identification, obtain information on the purpose and intended nature of the business relationship, where applicable;

(b) take reasonable steps to understand the nature of the customer's business, and its ownership and control; and

(c) determine whether a client is acting on behalf of a beneficial owner, and identify the beneficial owner and take all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification:

Provided that where the Regulator is of the view that money laundering and terrorist financing risks are effectively managed and where this is essential not to interrupt the normal conduct of business, the Regulator may permit the reporting entity to complete the verification as soon as reasonably practicable following the establishment of the relationship; and

Provided that where a client is subscribing or dealing with depository receipts or equity shares, issued or listed in jurisdictions notified by the Central Government, of a company incorporated in India, and it is acting on behalf of a beneficial owner who is a resident of such jurisdiction, the determination, identification and verification of such beneficial owner, shall be as per the norms of such jurisdiction and nothing in the sub-rules (3) to (9) of these rules shall be applicable for due-diligence of such beneficial owner.

Explanation-For the purposes of this proviso, the expression "equity share" means a share in the equity share capital of a company and equity share capital shall have the same meaning as assigned to it in the Explanation to section 43 of the Companies Act, 2013.

(1A) Subject to the provisions of sub-rule (1), every reporting entity shall within ten days after the commencement of an account-based relationship with a client, file the electronic copy of the client's KYC records with the Central KYC Records Registry[21];

[21]Central KYC Records Registry" means a reporting entity, substantially owned and controlled by the Central Government, and authorised by that Government through a notification in the Official Gazette to receive, store, safeguard and retrieve the KYC records in digital form of a client as referred to in clause (ha) in such manner and to perform such other functions as may be required under the PMLR. Further, as per IFSCA AML, CFT and KYC Guidelines, the Central KYC Records Registry is authorised to receive, store, safeguard and retrieve the KYC records of a customer in digital form.

(1B) The Central KYC Records Registry shall process the KYC records received from a reporting entity for de-duplicating and issue a KYC Identifier[22] for each client to the reporting entity, which shall communicate the KYC Identifier in writing to their client;

(1C) For the purpose of verification of identity of a client, under clause (a) and (b) of sub-rule (1) of Rule 9 or on-going due diligence as per clause (iii) of sub-rule (12), the reporting entity shall seek the KYC Identifier from the client or retrieve the KYC Identifier, if available, from the Central KYC Records Registry and proceed to obtain KYC records online by using such KYC Identifier and shall not require a client to submit the same KYC records or information or any other additional identification documents or details, unless—

i. there is a change in the information of the client as existing in the records of Central KYC Records Registry;
ii. the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms prescribed by the respective regulator; or
iii. the reporting entity considers it necessary in order to verify the identity or address (including current address) as per the guidelines issued by the regulator under sub-rule (14), or to perform enhanced due diligence or to build an appropriate risk profile of the client.

(1D) A reporting entity after obtaining additional or updated information from a client under sub-rule (IC), shall within seven days or within such period as may be notified by the Central Government furnish the updated information to the Central KYC Records Registry which shall update the existing KYC records of the client and the Central KYC Records Registry shall thereafter inform electronically all reporting entities who have dealt with the concerned client regarding updation of KYC record of the said client;

(1E) The reporting entity which performed the last KYC verification or sent updated information in respect of a client shall be responsible for verifying the authenticity of the identity or address of the client;

(1F) A reporting entity shall not use the KYC records of a client obtained from the Central KYC Records Registry for purposes other than verifying the identity or address of the client and shall not transfer KYC records or any information contained therein to any third party unless authorised to do so by the client or by the Regulator or by the Director;

(1G) The regulator shall issue guidelines to ensure that the Central KYC records are accessible to the reporting entities in real time.

[22]Know Your Client (KYC) Identifier" means the unique number or code assigned to a client/customer by the Central Know Your Customer Records Registry.

(1H) If an update in the KYC record of an existing client is informed by the Central KYC Records Registry to a reporting entity under sub-rule (1-D), the reporting entity shall retrieve the updated KYC records from the Central KYC Records Registry and update the KYC record maintained by the reporting entity as per the guidelines issued by the regulator under sub-rule (14) and under clause (g) of sub-rule (2) of Rule 9-A.

(2) For the purpose of clause (a) of sub-rule (1), a reporting entity may rely on a third party subject to the conditions that-

(a) the reporting entity, immediately, obtains from the third party or from the Central KYC Records Registry records or the information of the client due diligence carried out by the third party.

(b) the reporting entity takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;

(c) the reporting entity is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the Act;

(d) the third party is not based in a country or jurisdiction assessed as high risk;

(e) the reporting entity is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable; and

(f) where a reporting entity relies on a third party that 1s part of the same financial group, the Regulator may issue guidelines to consider any relaxation in the conditions (a) to (d).

(3) The beneficial owner for the purpose of sub-rule (1) in the clause 1.3.3. of the IFSCA AML, CFT and KYC Guidelines is determined as under—

(a) where the client is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

Explanation. — For the purpose of this sub-clause—

- “Controlling ownership interest” means ownership of or entitlement to more than ten per cent of shares or capital or profits of the company;
- “Control” shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements

(b) where the client is a partnership firm, the beneficial owner is the natural person, who, whether acting alone or together, or through one or more juridical person, has ownership of/entitlement to more than ten percent of capital or profits of the partnership or who exercises control through other means.
Explanation - For the purpose of this clause, “Control” shall include the right to control the management or policy decision;

(c) where the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals;

(d) where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

(e) where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with ten percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and

(f) where the client or the owner of the controlling interest is an entity listed on a stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary of such listed entities, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

(4) Where the client is an individual, he shall for the purpose of sub-rule (1) submit to the reporting entity, -

(a) the Aadhaar number where,

(i) he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or

(ii) he decides to submit his Aadhaar number voluntarily to a banking company or any reporting entity notified under first proviso to sub-section (1) of section 11A of the Act; or

(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or

(ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any officially valid document (OVD[23]) or the equivalent e-document[24] thereof containing the details of his identity and address; and

(b) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and

(c) such other documents including in respect of the nature of business and financial status of the client, or the equivalent e-documents thereof as may be required by the reporting entity

(5) Notwithstanding anything contained in sub-rule (4) and as an alternative thereto, an individual who desires to open a small account in a banking company may be allowed to open such an account on production of a self-attested photograph and affixation of signature or thumb print, as the case may be, on the form for opening the account:

Provided that -

(i) the designated officer of the banking company, while opening the small account, certifies under his signature that the person opening the account has affixed his signature or thumb print, as the case may be, in his presence. However, if the individual is a prisoner in a jail, the signature or thumb print shall be affixed in presence of the officer in-charge of the jail and the said officer shall certify the same under his signature and the account shall remain operational on annual submission of certificate of proof of address issued by the officer in-charge of the jail.

(ii) a small account shall be opened only at Core Banking Solution linked banking company branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to a small account and that the stipulated limits on monthly and annual aggregate of transactions and balance in such accounts are not breached, before a transaction is allowed to take place.

[23](OVD meaning is provided in clause 1 (d) of the PMLR and 1.3.30 of the IFSCA AML, CFT and KYC Guidelines)

[24]As per PMLR, “equivalent e-document" means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the client as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

(iii) a small account shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months if the holder of such an account provides evidence before the banking company of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty-four months.

(iv) Notwithstanding anything contained in clause (iii), the small account shall remain operational between 1st April, 2020 and 30th June 2020 and such other periods as may be notified by the Central Government.

(v) the small account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high-risk scenarios, the identity of client shall be established as per the provisions of sub-rule (4):

(vi) foreign remittance shall not be allowed to be credited into a small account unless the identity of the client is fully established as per the provisions of sub-rule (4).

(6) Where the client is a company, it shall for the purposes of sub-rule (1) submit to the reporting entity one certified copy of the following documents or the equivalent e-documents thereof: -

(i) Certificate of incorporation
(ii) Memorandum and Articles of Association;
(iii) Permanent Account Number of the company;
(iv) a resolution from the Board of Directors, power of attorney granted to its managers, officers or employees, as the case may be, to transact on its behalf;
(v) such documents as are required for an individual under sub-rule (4) relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf;
(vi) the names of the relevant persons holding senior management position and;
(vii) the registered office and the principal place of its business, if it is different.

(7) Where the client is a partnership firm, it shall, for the purposes of sub-rule (1), submit to the reporting entity the certified copies of the following documents or the equivalent e-documents thereof, namely: -

i. registration certificate,
ii. partnership deed,

iii. Permanent Account Number of the partnership firm

iv. such documents as are required for an individual under sub-rule (4) relating to beneficial owner, managers, officers or employees, as the case may be, of the person holding an attorney to transact on its behalf; and

v. the names of all the partners and address of the registered office, and the principal place of its business, if it is different.

(8) Where the client is a trust, it shall, for the purposes of sub-rule (1) submit to the reporting entity one certified copy of the following documents, namely or the equivalent e-documents thereof: -

i. registration certificate,

ii. trust deed;

iii. Permanent Account Number or Form No.60 of the trust;

iv. such documents as are required for an individual under sub-rule (4) relating to beneficial owner, managers, officers or employees, as the case may be, of the person holding an attorney to transact on its behalf,

v. the names of the beneficiaries, trustees, settlor or and authors of the trust and the address of the registered office of the trust; and

vi. list of trustees and documents as are required for individuals under sub-rule (4) for those discharging roles as trustee and authorised to transact on behalf of the trust.

(9) Where the client is an unincorporated association or a body of individuals, it shall submit to the reporting entity one certified copy of the following documents or the equivalent e-documents thereof: -

(i) resolution of the managing body of such association or body of individuals;

(ii) power of attorney granted to him to transact on its behalf;

(iii) Permanent account number or Form No.60 of the unincorporated association or a body of individuals;

(iv) such documents as are required for an individual under sub-rule (4) relating to beneficial owner, managers, officers or employees, as the case may be, of the person holding an attorney to transact on its behalf; and

(v) such information as may be required by the reporting entity to collectively establish the existence of such association or body of individuals.

(9A) Every Banking Company or Financial Institution or intermediary, as the case may be, shall register the details of a client, in case of client being a non-profit organisation, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and a reporting entity has ended or the account has been closed, whichever is later.

(9B) Where the client has submitted any documents for the purpose of sub-rule (1), it shall submit to the reporting entity any update of such documents, for the purpose of updating the records mentioned under sub-rules (4), (5), (6), (7), (8) or (9), as the case may be, within 30 days of such updation.

(10) Where the client purports to act on behalf of juridical person or individual or trust, the reporting entity shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person.
In case of a trust, the reporting entity shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as specified in clause (b) of sub-rule (1) rule9.

(11) No reporting entity shall allow the opening of or keep any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified.

(12) It has following three clauses:
(i) Every reporting entity shall exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with the knowledge of the client, his business and risk profile and where necessary, the source of funds.
(ii) When there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained client identification data, the reporting entity shall review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship, as the case may be.
(iii) The reporting entity shall apply client due diligence measures also to existing clients on the basis of materiality and risk, and conduct due diligence on such existing relationships at appropriate times or as may be specified by the regulator, taking into account whether and when client due diligence measures have previously been undertaken and the adequacy of data obtained.

(13) Every reporting entity shall -
(i) carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic

areas, and products, services, transactions or delivery channels that is consistent with any national risk assessment conducted by a body or authority duly notified by the Central Government.

(ii) the risk assessment mentioned in clause (i) shall
  (a) be documented
  (b) consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied
  (c) be kept up to date; and
  (d) be available to competent authorities and self-regulating bodies.

(14) (i) The regulator shall issue guidelines incorporating the requirements of sub-rules (1) to (13), sub-rule (15) and sub-rule (17) and may prescribe enhanced or simplified measures to verify the client's identity taking into consideration the type of client, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved.

Explanation-For the purpose of this clause, simplified measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply or where the risk identified is not consistent with the national risk assessment.

(ia) The guidelines issued under clause (i) shall also include appropriate-

(A) exemptions, limitations and conditions and alternate and viable means of identification, to provide account based services to clients who are unable to undergo biometric authentication;
(B) relaxation for continued operation of accounts for clients who are unable to provide Permanent Account Number or Form No. 60; and
(C) exemption, limitations and conditions and alternate and viable means of identification, to provide account based services of clients who are unable to undergo Aadhaar authentication for receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016);

owing to injury, illness or infirmity on account of old age or otherwise, and such like causes.

(ii) Every reporting entity shall formulate and implement a Client Due Diligence Programme, incorporating the requirements of sub-rules (1) to (13) 23, sub-rule (15) and sub-rule (17) and guidelines issued under clause (i) and (ia).

(iii) the Client Due Diligence Programme shall include policies, controls and procedures, approved by the senior management, to enable the reporting entity to manage and mitigate the risk that have been identified either by the reporting entity or through national risk assessment.

(15) Where the client has submitted –

(a) his Aadhaar number under clause (a) of sub-rule (4) to the banking company or a reporting entity notified under first proviso to sub-section (1) of section 11A, such banking company or reporting entity shall carry out authentication of the client's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India;

(b) proof of possession of Aadhaar under clause (aa) of sub-rule (4) where offline verification can be carried out, the reporting entity shall carry out offline verification;

(c) an equivalent e-document of any officially valid document, the reporting entity shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo in the manner specified by the regulator.

(d) any officially valid document or proof of possession of Aadhaar number under clause (ab) of sub-rule (4) where offline verification cannot be carried out, the reporting entity shall carry out verification through digital KYC[25].

Further, for a period not beyond such date as may be notified for a class of reporting entity, instead of carrying out digital KYC, the reporting entity pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the officially valid document and a recent photograph where an equivalent e-document is not submitted.

Explanation. — Obtaining a certified copy by the reporting entity shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the client with the original and recording the same on the copy by the authorised officer of the reporting entity as per the provisions contained in the Act.

[25] As per PMLR, Digitial KYC means the capturing live photo of the client and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the reporting entity as per the provisions contained in the Act. *As per IFSCA AML, CFT and KYC Guidelines Digital KYC definition, the word client is replaced with customer and the word reporting entity is replaced with regulated entity.*

(16) Every reporting entity shall, where its client submits a proof of possession of Aadhaar Number containing Aadhaar number, ensure such client redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under sub-rule (15).

(17) (i) A client already having an account based relationship with a reporting entity, shall submit his Permanent Account Number or the equivalent e-documents thereof or Form No.60, on such date as may be notified by the Central Government, failing which the account shall temporarily cease to be operational till the time the Permanent Account Number or the equivalent e-documents thereof or Form No. 60 is submitted by the client:

Further, before temporarily ceasing operations for an account, the reporting entity shall give the client an accessible notice and a reasonable opportunity to be heard.

Explanation. – For the purpose of this clause, "temporary ceasing of operations" in relation to an account means the temporary suspension of all transactions or activities in relation to that account by the reporting entity till such time the client complies with the provisions of this clause;

(ii) if a client having an existing account based relationship with a reporting entity gives in writing to the reporting entity that he does not want to submit his Permanent Account Number or the equivalent e-documents thereof or Form No.60, as the case may be, the client's account with the reporting entity shall be closed and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the client in the manner as may be determined by the regulator.

(18) In case of officially valid document furnished by the client does not contain updated address, the following documents or the equivalent e-documents thereof shall be deemed to be officially valid documents for the limited purpose of proof of address: -

(a) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill)
(b) property or Municipal tax receipt
(c) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address
(d) letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation:

Further, the client shall submit updated officially valid document or the equivalent e-documents thereof with current address within a period of three months of submitting the above documents.

(19) Where a client has provided his Aadhaar number for identification under clause (a) of sub-rule (4) and wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the reporting entity.

Functions and obligations of the Central KYC Records Registry (Rule 9A)

(1) The Central Government shall within a period of one hundred and eighty days from the date of coming into force of the Prevention of Money-laundering (Maintenance of Records) Amendment Rules, 2015 set-up a Central KYC Records Registry having its own seal for the purpose of receiving, storing, safeguarding and retrieving electronic copies of KYC records obtained by the reporting entities from their clients in accordance with these rules. However in an International Financial Services Centre, no such receiving, storing, safeguarding and retrieving of records shall be required for a client who is a foreign national.

(2) The Central KYC Registry shall perform the following functions and obligations, namely: —

a) shall follow any operating instructions issued by the Regulator, consistent with the guidelines referred to in clause (g) and issue the same to implement the requirements of these rules;
b) shall be responsible for storing, safeguarding and retrieving the KYC records and making such records available online to reporting entities or Director.
c) shall take all precautions necessary to ensure that the electronic copies of KYC records are not lost, destroyed or tampered with and that sufficient back up of electronic records are available at all times at an alternative safe and secure place.
d) shall cause an annual audit of its controls, systems, procedures and safeguards and shall undertake corrective actions for deficiencies, if any.
e) shall provide information only to the reporting entities which are registered with it on payment of fees as specified by the regulator.
f) shall appoint a compliance officer who shall be responsible for monitoring the compliance of the Act, the rules made and the notifications issued thereunder and also the guidelines and instructions issued by the Central Government and the Regulator and for redressal of client's grievances. The compliance officer shall immediately and independently report to the Central Government any noncompliance observed by him.

g) the Regulator in consultation with the Central Government and the Central KYC Records Registry may issue guidelines to be followed by the reporting entities for filing the KYC records with the Central KYC Records Registry.
h) the Central Government, in consultation with Regulator, may by notification in the public interest and in the interest of the regulated entities, direct that any of the provisions of rule 9 or rule 9A, —
   (i) shall not apply to a class or classes of regulated entities.
   (ii) shall apply to the class or classes of regulated entities with exceptions, modifications and adaptations.

3.3 Digital Know Your Customer (KYC) Procedure

A. The reporting entities shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated Application of the Reporting Entities.

B. The access of the Application shall be controlled by the Reporting Entities and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by Reporting Entities to its authorized officials.

C. The client, for the purpose of KYC, shall visit the location of the authorized official of the Reporting Entity or vice-versa. The original Officially Valid Document (OVD) shall be in possession of the client.

D. The Reporting Entity must ensure that the Live photograph of the client is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the Reporting Entity shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by Reporting Entities) and Date (DD:MM: YYYY) and time stamp (HH:MM: SS) on the captured live photograph of the client.

E. The Application of the Reporting Entities shall have the feature that only live photograph of the client is captured and no printed or video-graphed photograph of the client is captured. The background behind the client while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the client.

F. Similarly, the live photograph of the original officially valid document or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

G. The live photograph of the client and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

H. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the client. In those documents where, Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

I. Once the above-mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to client's own mobile number. Upon successful validation of the OTP, it will be treated as client signature on CAF. However, if the client does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officers registered with the Reporting Entity shall not be used for client signature. The Reporting Entity must check that the mobile number used in client signature shall not be the mobile number of the authorized officer.

J. The authorized officer shall provide a declaration about the capturing of the live photograph of client and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the Reporting Entity. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

K. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the Reporting Entity, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to client for future reference.

L. The authorized officer of the Reporting Entity shall check and verify that: -
   i. information available in the picture of document is matching with the information entered by authorized officer in CAF.
   ii. live photograph of the client matches with the photo available in the document.; and
   iii. all of the necessary details in CAF including mandatory field are filled properly.

M. On Successful verification, the CAF shall be digitally signed by authorized representative of the Reporting Entity who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

Sample Questions

1. After an Act has been passes and approved, its subsequent rules are made for what purpose?
   a) To define how the Act will be implemented
   b) To state how the Act will be performed
   c) To provide flexibility in the implementation of the Act
   d) All of the above

2. The PML (Maintenance of Records) Rules, 2005 require the reporting entities to take which of the following actions?
   a) Report suspicious transactions and other specified activities
   b) Ignore suspicious transactions and other specified activities
   c) Delay suspicious transactions and other specified activities
   d) None of these

3. Every reporting entity shall maintain the record of all cash transactions of value more than a specified amount or its equivalent in foreign currency. What is this specified/threshold amount?
   a) 5 lacs
   b) 10 lacs
   c) 20 lacs
   d) 25 lacs

4. For the purpose of receiving, storing, safeguarding and retrieving electronic copies of KYC records, within how many days of coming into force of the Prevention of Money-laundering (Maintenance of Records) Amendment Rules, 2005, a Central KYC Records Registry had to be set up?
   a) 100 days
   b) 150 days
   c) 180 days
   d) 200 days

Chapter-4 Scheduled Offences

Learning Objective- After studying this chapter, you should know about:

- scheduled offenses described under the IPC and BNS.

4.1 The Concept of Offence

The term offence is better known as "a crime or an illegal action". In order to proceed against a person under the PMLA, a scheduled offence, as defined under section 2(1)(y) and mentioned in Parts A, B and C of the Schedule of the PMLA 2002 should have been committed and the proceeds of crime should have been generated. A critical element, for an offence to be termed as a money laundering offence is the commission of a scheduled offence, as it serves as the foundation for generating proceeds of crime.

The offence of money laundering arises from criminal activity committed by a person in relation to scheduled offences. Scheduled offences (as defined in section 2(1)(y) of the PML Act) are those offences that are mentioned in Parts A, B and C of the Schedule to the PML Act and refer to any type of property or assets derived from proceeds of crime or used in the commission of crime in relation with the scheduled offences.

4.2 List of Scheduled Offences

Part A of the PMLA delineates an exhaustive list of scheduled offences drawn from various criminal legislations in India, including but not limited to the:

- Bharatiya Nyaya Sanhita (BNS) 2023 (erstwhile Indian Penal Code 1860),
- Narcotic Drugs and Psychotropic Substances Act 1985,
- Unlawful Activities (Prevention) Act 1967,
- Arms Act 1959,
- Prevention of Corruption Act 1988, and others, for which no monetary threshold has been provided.
- Antiquities and Art Treasures Act
- Copyright Act
- Trademark Act
- Wildlife Protection Act
- Information Technology Act

In addition to offences mentioned in Part A, **Part B** also encompasses offences under Indian tax laws, such as the Customs Act 1962, for which a monetary threshold of 3 million rupees or 10 million rupees has been prescribed as may be applicable.

Further, **Part C** of the PMLA specifies that any offence mentioned under Part A, particularly offences with cross-border implications, falls within the purview of the Act for which no monetary threshold has been provided.

List of scheduled offences is as follows[26]:

PART A		
Paragraph 1		
Offences Under the Indian Penal Code (45 of 1860) and under Bharatiya Nyaya Sanhita (BNS) 2023 (45 of 2023)		
Section under IPC	**Section under BNS**	**Description of Offence**
120 B	61(2)	Criminal conspiracy.
121	147	Waging, or attempting to wage war or abetting waging of war, against the Government of India.
121A	148	Conspiracy to commit offences punishable by section 121 against the State
255	178	Counterfeiting Government stamp.
257	181	Making or selling instrument for counterfeiting Government stamp.
258	179	Sale of counterfeiting Government stamp.
259	180	Having possession of counterfeit Government stamp.
260	179	Using as genuine a government stamp known to be counterfeit.
302	103(1)	Murder
304	105	Punishment for culpable homicide not amounting to murder.
307	109	Attempt to murder.
308	110	Attempt to commit culpable homicide.
327	119(1)	Voluntarily causing hurt to extort property, or to constrain to an illegal act.
329	119(2)	Voluntarily causing grievous hurt to extort property, or to constrain to an illegal act.
364A	140(2)	Kidnapping for ransom, etc.
384 to 389	308	Offences relating to extortion

[26]https://fiuindia.gov.in/files/AML_Legislation/scheduled_offences.html

392 to 402	310 - 313	Offences relating to robbery and dacoity.
411	317(2)	Dishonestly receiving stolen property.
412	317(3)	Dishonestly receiving property stolen in the commission of a dacoity.
413	317 (4)	Habitually dealing in stolen property.
414	317(5)	Assisting in concealment of stolen property.
417	318 (2)	Punishment for cheating.
418	318 (3)	Cheating with knowledge that wrongful loss may ensure to person whose interest offender is bound to protect.
419	319 (2)	Punishment for cheating by personation.
420	318 (4)	Cheating and dishonesty inducing delivery of properties
421	320	Dishonest or fraudulent removal or concealment of property to prevent distribution among creditors.
422	321	Dishonestly or fraudulently preventing debt being available for creditors.
423	322	Dishonest or fraudulent execution of deed of transfer containing false statement of consideration.
424	323	Dishonest or fraudulent removal or concealment of property.
467	338	Forgery of a valuable security, will, etc.
471	340(2)	Using as genuine a forged document or electronic record.
472 and 473	341 (1) & (2)	Making or possessing counterfeit seal, etc. with intent to commit forgery.
475 and 476	342	Counterfeiting device or mark.
481	345(2)	Using a false property mark.
482	345 (3)	Punishment for using false property mark.
483	347 (1)	Counterfeiting a property mark used by another.
484	347 (2)	Counterfeiting a mark used by a public servant.
485	348	Making or possession of any instrument for counterfeiting a property mark.
486	349	Selling goods marked with a counterfeit property mark.
487	350 (1)	Making a false mark upon any receptacle containing goods.
488	350 (2)	Punishment for making use of false mark.;
489A	178	Counterfeiting currency notes or bank notes.
489B	179	Using as genuine, forged or counterfeit currency notes or bank notes

Paragraph 2	
Offences under The Narcotic Drugs and Psychotropic Substances Act, 1985 (61 of 1985)	
Section	**Description of Offence**
15	Contravention in relation to poppy straw.
16	Contravention in relation to coca plant and coca leaves.
17	Contravention in relation to prepared opium.
18	Contravention in relation to opium poppy and opium
19	Embezzlement of opium by cultivator
20	Contravention in relation to cannabis plant and cannabis.
21	Contravention in relation to manufactured drugs and preparations
22	Contravention in relation to psychotropic substances
23	Illegal import into India, export from India or transhipment of narcotic drugs and psychotropic substances.
24	External dealings in narcotic drugs and psychotropic substances in contravention of section 12 of the Narcotics Drugs and Psychotropic Substances Act, 1985.
25A	Contravention of orders made under section 9A of the Narcotic Drugs and Psychotropic Substances Act, 1985
27A	Financing illicit traffic and harbouring offenders.
29	Abetment and criminal conspiracy.

Paragraph 3	
The Explosive Substances Act, 1908 (6 of 1908)	
Section	**Description of Offence**
3	Causing explosion likely to endanger life or property.
4	Attempt to cause explosion, or for making or keeping explosives with intent to endanger life or property.
5	Making or possessing explosives under suspicious circumstances.

Paragraph 4	
The Unlawful Activities (Prevention) Act, 1967 (37of 1967)	
Section	**Description of Offence**
10 read with section 3	Penalty for being member of an unlawful association, etc.
11 read with sections 3 and 7	Penalty for dealing with funds of an unlawful association
13 read	Punishment for unlawful activities.

with section 3	
16 read with section 15	Punishment for terrorist act
16A	Punishment for making demands of radioactive substances, nuclear devices, etc.
17	Punishment for raising fund for terrorist act.
18	Punishment for conspiracy, etc.
18A	Punishment for organising of terrorist camps.
18B	Punishment for recruiting of any person or persons for terrorist act
19	Punishment for harbouring, etc.
20	Punishment for being member of terrorist gang or organization.
21	Punishment for holding proceeds of terrorism.
38	Offence relating to membership of a terrorist organization.
39	Offence relating to support given to a terrorist organization
40	Offence for raising fund for a terrorist organization

Paragraph 5	
The Arms Act, 1959	
Section	**Description of Offence**
25	To manufacture, sell, transfer, convert, repair or test or prove or expose or offer for sale or transfer or have in his possession for sale, transfer, conversion, repair, test or proof, any arms or ammunition in contravention of section 5 of the Arms Act, 1959
	To acquire, have in possession or carry any prohibited arms or prohibited ammunition in contravention of section 7 of the Arms Act, 1959.
	Contravention of section 24A of the Arms Act, 1959 relating to prohibition as to possession of notified arms in disturbed areas, etc.
	Contravention of section 24B of the Arms Act, 1959 relating to prohibition as to carrying of notified arms in or through public places in disturbed areas.
	Other offences specified in section 25.
26	To do any act in contravention of any provisions of section 3, 4, 10 or 12 of the Arms Act, 1959 in such manner as specified in sub-section (1) of section 26 of the said Act etc.
	To do any act in contravention of any provisions of section 5, 6, 7 or section 11 of the Arms Act, 1959 in such manner as specified in sub-section (2) of section 26 of the said Act.
	Other offences specified in section 26.

27	Use of arms or ammunitions in contravention of section 5 or use of any arms or ammunition in contravention of section 7 of the Arms Act, 1959.
28	Use and possession of fire arms or imitation fire arms in certain cases.
29	Knowingly purchasing arms from unlicensed person or for delivering arms, etc., to person not entitled to possess the same.
30	Contravention of any condition of a licence or any provisions of the Arms Act, 1959 or any rule made thereunder.

Paragraph 6

The Wild Life (Protection) Act, 1972 (53 of 1972)

Section	**Description of Offence**
51 read with section 9	Hunting of wild animals
51 read with section 17A	Contravention of provisions of section 17A relating to prohibition of picking, uprooting, etc., of specified plants.
51 read with section 39	Contravention of provisions of section 39 relating to wild animals, etc., to be Government property.
51 read with section 44	Contravention of provisions of section 44 relating to dealings in trophy and animal articles without licence prohibited.
51 read with section 48	Contravention of provisions of section 48 relating to purchase of animal, etc., by licensee
51 read with section 49B	49B Contravention of provisions of section 49B relating to prohibition of dealings in trophies, animal articles etc., derived from scheduled animals.

Paragraph 7

The Immoral Traffic (Prevention) Act, 1956 (104 of 1956)

Section	**Description of Offence**
5	Procuring, inducing or taking person for the sake of prostitution.
6	Detaining a person in premises where prostitution is carried on.
8	Seducing or soliciting for purpose of prostitution.
9	Seduction of a person in custody.

Paragraph 8	
The Prevention of Corruption Act, 1988 (49 of 1988)	
Section	**Description of Offence**
7	Public servant taking gratification other than legal remuneration in respect of an official act.
8	Taking gratification, in order, by corrupt or illegal means, to influence public servant.
9	Taking gratification, for exercise of personal influence with public servant.
10	Abetment by public servant of offences defined in section 8 or section 9 of the Prevention of Corruption Act, 1988
13	Criminal misconduct by a public servant.;

Paragraph 9	
The Explosives Act, 1884 (4 of 1884)	
Section	**Description of Offence**
9-B	Punishment for certain offences
9-C	Offences by Companies.
25 read with section 3	Contravention of export trade in antiquities and art treasure.
28	Offences by Companies.
25 read with section 3	Contravention of export trade in antiquities and art treasure

Paragraph 10	
The Antiquities and Arts Treasures Act, 1972 (52 of 1972)	
Section	**Description of Offence**
25 read with section 3	Contravention of export trade in antiquities and art treasure.
28	Offences by Companies.

Paragraph 11	
The Securities and Exchange Board of India Act, 1992 (15 of 1992)	
Section	**Description of Offence**
12A read with section 24	Prohibition of manipulative and deceptive devices, insider trading and substantial acquisition of securities or control.
24	Acquisition of Securities or Control.

Paragraph 12	
The Customs Act, 1962 (52 of 1962)	
Section	**Description of Offence**
135	Evasion of duty or prohibitions

Paragraph 13	
The Bonded Labour System (Abolition) Act, 1976 (19 of 1976)	
Section	**Description of Offence**
16	Punishment for enforcement of bonded labour.
18	Punishment for extracting bonded labour under the bonded labour system.
20	Abetment to be an offence.

Paragraph 14	
The Child Labour (Prohibition and Regulation) Act, 1986 (61 of 1986))	
Section	**Description of Offence**
14	Punishment for employment of any child to work in contravention of the provisions of section 3.

Paragraph 15	
The Transplantation of Human Organs Act, 1994 (42 of 1994)	
Section	**Description of Offence**
18	Punishment for removal of human organ without authority.
19	Punishment for commercial dealings in human organs.
20	Punishment for contravention of any other provision of this Act.

Paragraph 16	
The Juvenile Justice (Care and Protection of Children) Act,2000 (56 of 2000)	
Section	**Description of Offence**
23	Punishment of cruelty to juvenile or child.
24	Employment of juvenile or child for begging.
25	Penalty for giving intoxicating liquor or narcotic drug or psychotropic substance to juvenile or child.
26	Exploitation of juvenile or child employee.

Paragraph 17	
The Emigration Act,1983 (31 of 1983)	
Section	**Description of Offence**
24	Offences and penalties.

Paragraph 18	
The Passport Act,1967 (15 of 1967)	
Section	**Description of Offence**

12	Offences and penalties.
Paragraph 19	
The Foreigners Act,1946 (31 of 1946)	
Section	**Description of Offence**
14	Penalty for contravention of provisions of the Act, etc.
14B	Penalty for using forged passport.
14C	Penalty for abetment
Paragraph 20	
The Copyright Act,1957 (14 of 1957)	
Section	**Description of Offence**
63	Offence of infringement of copyright or other rights conferred by this Act.
63A	Enhanced penalty on second and subsequent convictions.
63B	Knowing use of infringing copy of computer programme.
68A	Penalty for contravention of section 52A.
Paragraph 21	
The Trade Marks Act,1999 (47 of 1999)	
Section	**Description of Offence**
103	Penalty for applying false trademarks, trade description, etc.
104	Penalty for selling goods or providing services to which false trademark or false trade description is applied.
105	Enhanced penalty on second or subsequent conviction.
107	Penalty for falsely representing a trade mark as registered.
120	Punishment of abetment in India of acts done out of India.
Paragraph 22	
The Information Technology Act, 2000 (21 of 2000)	
Section	**Description of Offence**
72	Penalty for breach of confidentiality and privacy.
75	Act to apply for offence or contravention committed outside India
Paragraph 23	
The Biological Diversity Act,2002 (18 of 2003)	
Section	**Description of Offence**
55 read with 6	Penalties for contravention of section 6, etc.
Paragraph 24	
The Protection of Plant Varieties and Farmers' Rights Act,2001 (53 of 2001)	
Section	**Description of Offence**

70 read with section 68	Penalty for applying false denomination, etc.
71 read with section 68	Penalty for selling varieties to which false denomination is applied.
72 read with section 68	Penalty for falsely representing a variety as registered.
73 read with section 68	Penalty for subsequent offence.
Paragraph 25	
The Environment Protection Act,1986 (29 of 1986)	
Section	**Description of Offence**
15 read with section 7	Penalty for discharging environmental pollutants.
15 read with section 8	Penalty for handling hazardous substance.
Paragraph 26	
The Water (Prevention and Control of Pollution) Act,1974 (6 of 1974)	
Section	**Description of Offence**
41(2)	Penalty for pollution of stream or well.
43	Penalty for contravention of provisions of section 24.
Paragraph 27	
The Air (Prevention and Control of Pollution) Act,1981 (14 of 1981)	
Section	**Description of Offence**
37	Failure to comply with the provisions for operating industrial plant.
Paragraph 28	
The Suppression of Unlawful Acts Against Safety of Maritime Navigation and Fixed Platforms on Continental Shelf Act, 2002 (69 of 2002)	
Section	**Description of Offence**
3	Offences against ship, fixed platform, cargo of a ship, maritime navigational facilities, etc.
Paragraph 29	

Offence under the Companies Act, 2013	
Section	**Description of Offence**
447	Punishment for fraud

PART B	
OFFENCE UNDER THE CUSTOMS ACT, 1962	
Section	**Description of Offence**
132	False declaration, false documents, etc.

PART C
An offence which is the offence of cross border implications and is specified in, —
(1) Part A; or
(3) the offences against property under Chapter XVII of the Indian Penal Code.
(4) The offence of the wilful attempt to evade any tax, penalty or interest referred to in section 51of the Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, 2015.

Sample Questions

1. Under the Prevention of Money Laundering Act, 2002, which of the following is a mandatory pre-condition for initiating proceedings for the offence of money laundering?
   a) Registration of an FIR under any cognizable offence
   b) Detection of suspicious transaction by a reporting entity
   c) Commission of a scheduled offence listed in Parts A, B or C of the Schedule and generation of proceeds of crime
   d) Issuance of a show-cause notice by FIU-IND

2. Which of the following best describes the relationship between scheduled offences and the offence of money laundering under PMLA?
   a) Scheduled offences are independent crimes and have no linkage with money laundering prosecution
   b) Money laundering offence can be established even without commission of a scheduled offence
   c) Scheduled offences form the foundation for money laundering as they generate proceeds of crime
   d) Scheduled offences apply only to cross-border crimes listed under Part C of the Schedule

3. Which of the following will be considered as a money laundering offence?
   a) Contravention in relation to cannabis plant and cannabis.
   b) Contravention in relation to manufactured drugs and preparations
   c) Contravention in relation to psychotropic substances
   d) All of the above

4. Offences under Bharatiya Nyaya Sanhita (BNS) 2023 are covered under which part of scheduled offences?
   a) Part A of the Schedule.
   b) Part B of the Schedule
   c) Part C of the Schedule
   d) All of the above

Part B: IFSCA Regulations for Anti Money Laundering (AML), Counter-Terrorist Financing (CTF) and Know Your Customer (KYC)

Chapter-5 IFSCA (Anti Money Laundering, Counter Terrorist Financing and Know Your Customer) Guidelines, 2022

Learning Objective- After studying this chapter, you should know about:

- The Duties of a Regulated Entity (RE)
- The Risk Based Approach to be adopted by the RE
- Adoption of the Business Risk Assessment by RE
- Aspects of Customer Due Diligence, Reporting of Suspicious Transactions, Record Keeping etc. by RE.

5.1 Introduction of IFSCA (AML, CFT and KYC) Guidelines

International Financial Services Centres Authority (IFSCA) has implemented several initiatives to combat money laundering, including the IFSCA Anti Money Laundering (AML), Counter Terrorist Financing (CFT)[27] and Know Your Customer (KYC) Guidelines. The abbreviated form of the guidelines is IFSCA (AML, CFT and KYC) Guidelines, 2022. These guidelines mandate regulated entities to establish robust AML frameworks to detect and report suspicious transactions related to money laundering and terrorist financing. Key aspects of these initiatives include customer due diligence, risk assessment, enhanced due diligence for high-risk customers, record-keeping, and reporting of suspicious transactions. Additionally, IFSCA conducts both onsite and offsite supervision of regulated entities to ensure compliance with AML/CFT regulations.

These Guidelines have been divided in 12 chapters highlighting different aspects, few of which have already been covered under previous chapters

1) Chapter-I - Applicability, Definitions and Responsibilities
2) Chapter-II - Risk-Based Approach
3) Chapter-III - Business Risk Assessment
4) Chapter-IV Customer Risk Assessment
5) Chapter-V Customer Due Diligence
6) Chapter-VI Third Party Reliance
7) Chapter-VII Correspondent Banking and Wire Transfer
8) Chapter-VIII Internal Policies, Compliance, Audit and Training
9) Chapter-IX Record Keeping

[27] In the IFSC domain, CFT and CTF are interchangeably used as the abbreviated forms of Counter Terrorist Financing.

10) Chapter-X Process of Identification and reporting of Suspicious Transactions
11) Chapter-XI Compliance obligations under International Agreements and domestic laws
12) Chapter-XII Groups, Branches and Subsidiaries

5.2 Duties of a Regulated Entity

As per IFSCA (AML, CFT and KYC) Guidelines, a Regulated Entity means a unit/entity which has been granted license, recognition, registration or authorisation by the Authority. The duties of a Regulated Entity are:

(a) Every Regulated Entity shall formulate an AML-CFT policy, which shall be duly approved by the Governing Body or by a committee to whom such power has been delegated by the Governing Body. While formulating the AML-CFT policy, every Regulated Entity shall incorporate the key principles or elements of these Guidelines.

(b) Additionally, every Regulated Entity shall develop a KYC Policy which shall be the part of its AML-CFT policy.

(c) Every member of Regulated Entity's Senior Management shall be responsible for the Regulated Entity's compliance under these Guidelines. While carrying out their responsibilities under these Guidelines every member of a Regulated Entity's Senior Management shall exercise due skill, care, and diligence.

5.3 Risk Based Approach[28]

The Chapter II if the IFSCA (AML, CFT and KYC) Guidelines, describes the Risk-based Approach to be adopted by the regulated entities, in the following manner:

(a) The primary thrust of these guidelines is to enable a Regulated Entity to adopt Risk-Based Approach (RBA) to identify and assess the Money Laundering (ML) and Terrorist Financing (TF) risk to which the Regulated Entity is exposed, depending upon its nature of business and exposure to or involvement with certain types of clients, countries or geographic areas, products, services, transactions, or delivery channels, etc. and document the same.

A Regulated Entity while adopting RBA shall ensure that:

i. The RBA is objective and proportionate to the risks;
ii. The RBA is based on reasonable grounds; and

[28] The RBA should be an essential foundation in Regulated Entity's AML-CFT compliance culture, and it must trickle down from the level of Senior Management to the rest of the organization.

iii. The RBA is reviewed and updated at appropriate intervals

(b) The RBA shall be appropriate to the nature and size of the business. While implementing the RBA, the Regulated Entity shall consider all relevant risk factors before deciding overall risk. Based on the risk assessment, the Regulated Entity shall monitor, manage, and mitigate the risks it is exposed to by applying effective, appropriate and proportionate measures.

(c) In addition to assessing the ML/TF risks presented by an individual customer, a Regulated Entity shall also identify and assess ML/TF risks at an enterprise-wide level, Financial Group-wide level or Group-wide level, wherever applicable. This shall include a consolidated assessment of the Regulated Entity's ML/TF risks perception that exist across all its business units, product lines and delivery channels.[29]

(d) The outcome of the risk assessment by a Regulated Entity shall be properly documented. The documentation should include:

- the enterprise-wide AML/CFT risk assessment wherever applicable,
- details of the implementation of the AML/CFT risk management systems, and
- controls as guided by the AML/CFT risk assessment.

A Regulated Entity shall ensure that the ML/TF risk assessment information are made available to the Authority upon request.

The records of documented risk assessment shall be kept as per the requirements of record keeping process specified under these Guidelines.

(e) The result of the risk assessment shall be used to classify the ML/TF risks as low, medium, and high. The general principle of this classification is to apply enhanced measures in case of high-risk customers and simplified measures in case of low-risk customers.

(f) To keep the risk assessments up-to-date, the Regulated Entity shall review its risk assessment at least once every two years or when a material trigger event occurs, whichever is earlier. The outcome of the exercise shall be put up to the Governing Body or such other committee of the Regulated Entity to which power in this regard has been delegated.

[29] Explanation: FATF Public Statement, the reports and guidance notes on AML/CFT/PF issued by FATF and any country specific information that is circulated by relevant authorities from time to time, as well as the updated list of natural and legal persons who are subjected to sanction measures as required under various United Nations' Security Council Resolutions. etc., may also be used in risk assessment.

5.4 Business Risk Assessment

The Chapter III of the IFSCA (AML, CFT and KYC) Guidelines describes that a regulated entity shall adopt a business risk assessment. It shall take into consideration the nature, size and the complexity of its business activities and take suitable steps to identify its exposure to ML/TF risks. It should consider the following risk factors, to the extent applicable and relevant, while identifying and assessing the ML/TF risks:

(i) its type of customers and their activities;
(ii) its business engagement with the countries or geographic areas;
(iii) its products, services, delivery channels and activity profiles;
(iv) the complexity and volume of its transactions;
(v) the development of new products and new business practices, including new delivery mechanisms, channels and partners; and
(vi) the use of new or developing technologies for both new and pre-existing products;

Further, based on the assessment and risk identification made as per clauses above, the Regulated Entity shall undertake commensurate mitigation measures.

5.4.1 New products, business practices and technologies

A Regulated Entity shall identify and assess the ML and TF risks that may arise in relation to: -

i. the development of new products, business practices, including new delivery mechanisms; and
ii. the use of new or developing technologies for both new and pre-existing products.

The Regulated Entity shall undertake the above risk assessment exercise, prior to the launch or use of such products, practices and technologies and shall take appropriate measures to manage and mitigate the risks.

5.4.2 AML/CFT systems and controls:

The nature and extent of AML/CFT systems and controls implemented by a Regulated Entity shall be commensurate with the ML/TF risks identified via the enterprise-wide ML/TF risk assessment, wherever applicable. A Regulated Entity shall put in place adequate policies, procedures, systems and controls to mitigate such ML/TF risks. The information obtained from the risk assessment shall be used to:

i. establish and maintain effective policies, procedures, systems and controls to prevent ML/TF;
ii. ensure that Regulated Entity’s AML/CFT policies, procedures, systems and controls adequately mitigate the risks identified above;

iii. ensure that Regulated Entity's systems and controls:
   a) include a provision enabling its Senior Management to regularly review the information on operations and effectiveness of its AML systems and controls;
   b) enable the Regulated Entity to determine:
      - whether a customer or a Beneficial Owner is a Politically Exposed Person (PEP)[30]; and
      - whether a beneficiary of the policy, or a Beneficial Owner of such beneficiary is a PEP, (in the cases where it is providing life insurance or other similar policies); and
      - enable a Regulated Entity to comply with these Guidelines and applicable AML-CFT legislations.

iv. ensure that regular risk assessments are carried out on the adequacy of the Regulated Entity's AML/CFT systems and controls to enable it to identify, assess, monitor, manage and mitigate such risks adequately.

The AML/CFT policies, procedures and controls shall be approved by Senior Management to enable a Regulated Entity to effectively manage and mitigate the risks either identified by it or notified to it by the Authority or other relevant authorities.

Further, the Regulated Entity shall constantly monitor the implementation of the policies, procedures and controls, and improve them, if necessary.

5.5 Identification and Reporting of Suspicious Transactions

5.5.1 Identification of Suspicious Transactions

As per PML Rules, Registered Intermediaries shall ensure that appropriate steps are taken to enable suspicious transactions to be recognized and have appropriate procedures for reporting suspicious transactions. While determining suspicious transactions, registered intermediaries shall be guided by the definition of a suspicious transaction contained in PML Rules as amended from time to time.

As per IFSCA (AML, CFT and KYC) Guidelines, the process of identification of suspicious transactions is described as follows:

I. Internal reporting requirements

A regulated entity shall:

(a) establish and maintain policies, procedures, systems and controls in order to monitor and detect suspicious transactions with respect to potential ML/TF.

[30]Politically Exposed Persons" (PEPs) are individuals who have been entrusted with prominent public functions by a foreign country, including the heads of States or Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.

(b) put in place such policies, procedures, systems and controls which ensure that whenever any of its employee, acting in the ordinary course of his employment, either:
   (i) knows;
   (ii) suspects; or
   (iii) has reasonable grounds for knowing or suspecting;

   that a person is engaged in or attempting ML/TF, that employee promptly notifies the Principal Officer of the Regulated Entity with all relevant details.

II. Indications of Suspicious Transactions

A Regulated Entity can identify suspicious transactions by following these four steps:

(a) Detect a suspicious indicator(s);
(b) Ask the customer questions;
(c) Review customer's records; and
(d) Evaluate the above information.

5.5.2 Reporting of Suspicious Transactions

A Regulated Entity shall establish and maintain policies, procedures, systems and controls in order to monitor and detect suspicious transactions with respect to potential money laundering and terrorist financing.

As per clause 10.3 of the IFSCA (AML, CFT and KYC) Guidelines, the reporting requirements of a regulated entity to Financial Intelligence Unit-India-IND are as follows:

A Regulated Entity shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), the required information referred to in rule-3 of the PML Rules and in accordance with the terms of rule-7 thereof.

The AML, CFT and KYC guidelines of IFSCA, further state that:

1) The reporting formats and comprehensive reporting format guide prescribed or released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist Regulated Entities in the preparation of prescribed reports shall be taken note of.
   The editable electronic utilities to file Suspicious Transaction Reports (STR) which FIU-IND has placed on its website, shall be made use of by Regulated Entities which are yet to install/adopt suitable technological tools for extracting STR from their live transaction data.

2) While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall constitute a separate violation.

3) Robust software to throw alerts when the transactions are inconsistent with risk categorization and updated profile of the customers, shall be put in to use as a part of effective identification and reporting of suspicious transactions.

4) In terms of the Rules, the Regulated Entities are mandated to report information relating to suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND,

Financial Intelligence Unit-India,

6th Floor, Tower-2,

Jeevan Bharati Building, Connaught Place,

New Delhi-110001, Telephone: 91-11-23314429, 23314459

Website: http://fiuindia.gov.in

5) The Regulated Entities shall carefully go through all the reporting requirements and formats that are available on the website of FIU – IND.

Further, in terms of Rules, the Regulated Entities shall inter-alia adhere to the following:

i. The Suspicious Transaction Report (STR) shall be submitted promptly on conclusion that any transaction or a series of transactions that are integrally connected, are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or relating to suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion.
ii. The Non-Profit Organization Transaction Reports (NTRs) for each month shall be submitted to FIU-IND by 15th of the succeeding month.
iii. The Principal Officer shall be responsible for timely submission of STR and NTR to FIU-IND;
iv. Utmost confidentiality shall be maintained in filing of STR and NTR to FIU-IND.

Further, as per the IFSCA (AML, CFT and KYC) Guidelines a regulated entity and its employees or agents are required to maintain the confidentiality of the STR in the manner prescribed by IFSCA from time to time.

Moreover, the lawyers, notaries, accountants, and entities offering services shall report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the following activities:

i. buying and selling of real estate;
ii. managing of client money, securities or other assets;
iii. management of bank, savings or securities accounts;
iv. organization of contributions for the creation, operation or management of companies;
v. creation, operation or management of legal persons or arrangements, and buying and selling of business entities

5.6 Correspondent Banking and Wire transfer

5.6.1 Correspondent Banking:

Correspondent banking is a banking arrangement where one bank (the correspondent bank) provides services to another bank (the respondent bank), typically to facilitate transactions in a foreign country. These services can include things like wire transfers, currency exchange, and trade finance. Essentially, the correspondent bank acts as an intermediary, enabling the respondent bank to offer services to its customers even if it doesn't have a direct presence in that market.

A Regulated Entity shall have a policy approved by its Governing Body, or by a committee headed by the Chairman/CEO/MD to lay down parameters for approving correspondent banking relationships subject to the following conditions namely: -

(a) assessment of the suitability of the respondent bank by taking the following steps:
    i. gather adequate information about the respondent bank to fully understand the nature of the respondent bank's business, including making appropriate inquiries on its management, its major business activities and the countries or jurisdictions in which it operates;
    ii. determine from the available sources, the reputation of the respondent bank and the quality of supervision over it, including whether it has been the subjected to any ML/TF investigation or regulatory action; and
    iii. assess the respondent bank's AML/CFT controls and ascertain whether they are adequate and effective, having regard to the AML/CFT measures of the country or jurisdiction in which the respondent bank operates.
(b) the responsibilities of each bank with whom correspondent banking relationship is established shall be clearly documented.
(c) obtain approval from the Senior Management before providing correspondent banking or similar services to a respondent bank.
(d) in the case of payable-through-accounts, the correspondent bank shall be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them.

(e) The correspondent bank shall ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.
(f) Correspondent relationship shall not be entered into with a bank which is a Shell Financial Institution.
(g) It shall be ensured that the correspondent banks do not permit their accounts to be used by bank which is a Shell Financial Institution.
(h) It shall be cautious with respondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.
(i) It shall be ensured that respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

5.6.2 Wire Transfers:

Wire Transfer means any transaction carried out on behalf of a Wire Transfer Originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a Beneficiary Institution, irrespective of whether the originator and the beneficiary are the same person.

A wire transfer is an electronic method of transferring money from one bank account to another, often used for both domestic and international transactions. It's a secure and relatively fast way to send money, especially for larger or urgent transactions like international payments or real estate deals.

1) This Clause shall apply to a bank or Regulated Entity when it sends funds by wire transfer or when it receives funds (including serial payments and cover payments) by wire transfer on the account of the wire transfer originator or the wire transfer beneficiary, but shall not apply to a transfer and settlement between the bank and another financial institution where the bank and the other financial institution are acting on their own behalf as the wire transfer originator and the wire transfer beneficiary, respectively.
   Further, the Regulated Entity shall verify the information pertaining to its customer where there is a suspicion of ML/TF. All Financial Institutions shall transact and receive all monetary consideration (i.e., funds/fees/amount) only through an account maintained with a Banking Unit in the IFSC.
2) A Regulated Entity shall monitor payment messages to and from high-risk countries or jurisdictions, as well as transactions with high risk countries or jurisdictions and suspend or reject payment messages or transactions with sanctioned parties or countries or jurisdictions.

3) Where name screening checks confirm that the wire transfer originator or wire transfer beneficiary is a terrorist or a terrorist entity, the Regulated Entity shall block, reject or freeze assets of these terrorists or terrorist entities immediately.
4) Where there are positive hits arising from name screening checks, they should be escalated to the Principal Officer. The decision to approve or reject the receipt or release of the wire transfer should be made at an appropriate level and be documented.
5) A Regulated Entity shall not omit, delete or alter information in payment messages, for the purpose of avoiding detection of that information by another Regulated Entity in the payment process.

Before effecting a wire transfer, every bank that is an ordering institution shall identify the wire transfer originator and verify his or its identity; and record adequate details of the wire transfer so as to permit its reconstruction, including but not limited to, the date of the wire transfer, the type and amount of currency transferred and the value date.

In a cross-border wire transfer where the amount to be transferred is below or equal to USD 1000, every bank which is an ordering institution shall include in the message or payment instruction that accompanies or relates to the wire transfer, the following:

i. the name of the wire transfer originator; the wire transfer originator's account number (or unique transaction reference number where no account number exists);
ii. the name of the wire transfer beneficiary; and
iii. the wire transfer beneficiary's account number (or unique transaction reference number where no account number exists).

If the amount to be transferred exceeds USD 1000, every bank which is an ordering institution shall include in the message or payment instruction that accompanies or relates to the wire transfer, the information required as above, and any of the following:

i. the wire transfer originator's residential address;
ii. registered or business address, and if different, principal place of business, as the case may be;
iii. the wire transfer originator's unique identification number (such as an identity card number, birth certificate number or passport number, or where the wire transfer originator is not a natural person, the incorporation number or business registration number); or
iv. the date and place of birth, incorporation or registration of the wire transfer originator (as applicable).

Additionally, in a cross-border wire transfer where the amount to be transferred is equal to USD 1000, every bank which is an ordering institution shall also comply with these requirements.

Where several individual cross-border wire transfers from a single wire transfer originator are bundled in a batch file for transmission to wire transfer beneficiaries, a bank shall ensure that the batch transfer file contains below information which are fully traceable within the beneficiary country:

i. the wire transfer originator information required under above Clause, which has been verified; and
ii. the wire transfer beneficiary information required under above Clause

Furthermore, these Guidelines shall apply to all Cross- Border Wire Transfers which are bundled in a batch file.

5.6.3 Responsibility of the Intermediary Institution

a) A bank, who is acting as an intermediary institution, shall retain all the required information related to wire transfer originator and wire transfer beneficiary, accompanying the wire transfer.
b) Where technical limitations prevent the required information related to wire transfer originator or wire transfer beneficiary accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record shall be preserved by the receiving intermediary institution for at least six years.
c) An intermediary institution shall implement appropriate internal risk-based policies, procedures and controls for determining-
   i. when to execute, reject, or suspend a wire transfer lacking required wire transfer originator or wire transfer beneficiary information; and
   ii. the appropriate follow-up actions

The Intermediary Institution shall be required to take all reasonable measures, consistent with straight-through processing, to identify cross-border wire transfers that lack the information required under the clause 7.7.6 (a) of the IFSCA (AML, CFT and KYC) Guidelines.

5.6.4 Domestic Wire Transfers

Domestic Wire Transfer" means a wire transfer where both the ordering institution and beneficiary institution are located in the IFSC and also refers to any chain of wire transfers that takes place entirely within the IFSC.

In a domestic wire transfer, every bank that is an ordering institution shall either: -

(a) include in the message or payment instruction that accompanies or relates to the wire transfer, the following:

i. the name of the wire transfer originator;
ii. the wire transfer originator's account number (or unique transaction reference number where no account number exists); and
iii. any of the following:

(aa) the wire transfer originator's residential or registered or business address or principal place of business (if registered and business addresses are different), as applicable;

(bb) the wire transfer originator's unique national identification number (such as an identity card number, birth certificate number or passport number, or where the wire transfer originator is not a natural person, the incorporation number or business registration number);

(cc) the date and place of birth, incorporation or registration of the wire transfer originator (as applicable).

(b) Include only the wire transfer originator's account number (or unique transaction reference number where no account number exists), provided: -

i. that these details will permit the transaction to be traced back to the wire transfer originator and wire transfer beneficiary;
ii. the ordering institution shall provide the wire transfer originator information set out in Clause (a) above, within 3 business days of a request for such information by the beneficiary institution, by the Authority or other relevant authorities; and
iii. the ordering institution shall provide the wire transfer originator information set out in Clause (a) above, immediately upon request for such information by law enforcement authorities in India.

(c) All wire transfer originator and beneficiary information collected by the ordering institution shall be documented. Where the ordering institution is unable to comply with the requirements under all of the Clauses above, it shall not execute the wire transfer.

5.7 Internal Policies, Compliance, Audit and Training

Internal Policies: A Regulated Entity shall develop and implement adequate internal policies, procedures, and controls, taking into consideration its ML/TF risks and the size of business, to help prevent ML/TF, and communicate these to its employees. As internal policies and procedures serve to guide employees, officers and representatives in ensuring compliance with AML/CFT laws and regulations, it is important that a Regulated Entity updates its policies and procedures in a timely manner, to take into account new operational, legal and regulatory developments and emerging or new ML/TF risks.

5.7.1 Compliance

A Regulated Entity shall develop appropriate compliance management, including appointing or designating a Principal Officer at the management level and shall also develop compliance framework. They shall ensure that the Principal Officer, as well as any other persons appointed to assist him, is suitably qualified and, has adequate resources and timely access to all customer records and other relevant information which he may require to discharge his functions. Further a Regulated Entity shall ensure that the Principal Officer has the necessary seniority and authority within the Regulated Entity to effectively perform his responsibilities. The responsibilities of the Principal Officer shall include:

i. carrying out, or overseeing the carrying out of, ongoing monitoring of business relations for compliance with these Guidelines;
ii. promoting compliance of these Guidelines and taking overall charge of all AML/CFT matters within the organisation;
iii. informing employees, officers and representatives promptly of regulatory changes;
iv. ensuring a speedy and appropriate reaction to any matter in which ML/TF is suspected;
v. reporting or overseeing the reporting of suspicious transactions;
vi. advising and training employees, officers and representatives on developing and implementing internal policies, procedures and controls on AML/CFT;
vii. reporting to Senior Management on the outcome of reviews of the Regulated Entity’s compliance with these Guidelines & risk assessment procedures; and
viii. reporting regularly on key AML/CFT risk management and control issues, and any necessary remedial actions, arising from audit, inspection & compliance reviews to the Regulated Entity’s Senior Management.

The business interests of a Regulated Entity should not interfere with the effective discharge of the above-mentioned responsibilities of the Principal Officer and potential conflicts of interest should be avoided.

To enable unbiased judgments and facilitate impartial advice to management, the Principal Officer should be distinct from the internal audit and business line functions. Where any conflict between business lines and the responsibilities of the Principal Officer arises, procedures should be in place to ensure that AML/CFT concerns are objectively considered and addressed at the appropriate level of the Regulated Entity’s management.

5.7.2 Audit

A Regulated Entity shall maintain an audit function that is adequately resourced and independent, that is able to regularly assess the effectiveness of the Regulated Entity's internal policies, procedures and controls, in compliance with regulatory requirements and these Guidelines. A Regulated Entity's AML/CFT framework should be subjected to periodic audits. Such audits should be performed not just on individual business functions but also on a Regulated Entity-wide basis. Auditors should assess the effectiveness of measures taken to prevent ML/TF. This would inter-alia include —

i. Determining the adequacy of the Regulated Entity's AML/CFT policies, procedures and controls, ML/TF risk assessment framework and application of risk-based approach;
ii. Reviewing the content and frequency of AML/CFT training programmes, and the extent of employee's, officer's and representative's compliance with established AML/CFT policies and procedures; and
iii. Assessing whether instances of non-compliance are reported to Senior Management on a timely basis. The frequency and extent of the audit should be commensurate with the ML/TF risks presented and the size and complexity of the Regulated Entity's business.

5.7.3 Training and awareness

The Regulated Entity shall provide AML/CFT training to all relevant employees, periodically. It shall ensure that its AML/CFT training enables its employees to:

i. comprehend the applicable laws relating to ML/TF, including the Act and Rules;
ii. understand its policies, procedures, systems and controls related to AML/CFT and any amendments/modifications thereto;
iii. recognise and deal with transactions and other activities which may be related to ML/TF;
iv. comprehend the kind of activity that may constitute suspicious activity, which warrants prompt notification to the Principal Officer;
v. have knowledge of the prevailing techniques, methods and trends in ML/TF, relevant to the business of the Regulated Entity;
vi. understand their roles and responsibilities in combating ML/TF, including the identity and duties of the Regulated Entity's Principal Officer and deputy, where applicable; and,
vii. understand the relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions

The regulated entity shall ensure that its AML/CFT training is relevant and tailored to the Regulated Entity's activities, including its products, services, customers, distribution channels, business partners, level and nature of its transactions and identifies and indicates the different levels of ML/TF risk and vulnerabilities associated with the matters as mentioned above.

5.7.4 Compliance obligations under International Agreements and domestic laws:

Requirements/obligations under International Agreements Communications from International Agencies – The Regulated Entities shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, they do not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists[31] are as under:

a) The "ISIL (Da'esh) &Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida.[32]
b) The "1988 Sanctions List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban.[33]

Details of accounts resembling any of the individuals/entities mentioned in the above lists, shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA Order bearing file no.14014/01/2019/CFT dated February 2, 2021, issued by the CTCR Division of the Ministry of Home Affairs, Government of India.[34]

In addition to the above, other UNSC Resolutions circulated by the IFSCA in respect of any other jurisdictions/ entities from time to time, shall also be taken note of for necessary compliances.

5.8 Record Keeping

A Regulated Entity shall maintain the following records:

a) a copy of all documents and information obtained in undertaking initial and ongoing Customer Due Diligence;
b) records of customer business relationships (both original and certified copies), which include: -
    i. correspondence of business and other information relating to a customer's account;
    ii. adequate records of transactions to enable standalone transactions to be reconstructed; and

---

[31] These are as per Chapter XI clause 11.1 of the IFSCA AML, KYC, CFT Regulations 2022.

[32] The updated ISIL &Al- Qaida Sanctions List is available at: https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xls

[33] The list is available at: https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl

[34] It is available at: https://www.mha.gov.in/sites/default/files/ProcedureImplementationSection51A_30032021.pdf

iii. internal findings and analysis relating to a business transaction or other transactions, where the transaction or business may be unusual or suspicious, whether or not it results in a Suspicious Transactions Report;

c) notifications made under Clause 10.1. (b);
d) Suspicious Transactions Reports and any relevant supporting documents and information, including internal findings and analysis;
e) any relevant communications, if made with the FIU;
f) the documents referred to in Clause 9.4; and
g) any other matter that the Regulated Entity may be expressly required to record and maintain, under these Guidelines.

The Regulated Entity shall preserve all necessary records, for at least six years or for such period as prescribed under the applicable laws, from the date on which business relationship has ended or transaction is completed. The Regulated Entity shall provide to the Authority or any law enforcement agency immediately on request, a copy of a records maintained by it under these Guidelines.

5.8.1 Risk Assessment Documents

A Regulated Entity shall keep and maintain all risk assessment documents and provide to the Authority immediately on request, all relevant documents and information, including: -

a) the business risk assessment undertaken by them;
b) how the business risk assessment in (a) was used for the purposes of complying with the guidelines
c) the risk assessment of its customer undertaken and,
d) the determination of risk rating

The above records may be kept in electronic format, subject to the condition that such records are readily accessible and promptly made available to the Authority or other law enforcement agency, on demand. Where the date on which the business relationship with a customer has ended remains unclear, it may be taken to have ended on the date of the completion of the last transaction. The Regulated Entity shall evolve a system for proper maintenance and preservation of records in such a manner that allows:

a) data to be retrieved easily and quickly whenever required or when demanded by the competent authorities;
b) the Authority or any other competent authority is able to assess the Regulated Entity's compliance with the applicable laws;
c) identification of a customer or third party;

d) it permits reconstruction of any transaction which was processed by or through the Regulated Entity on behalf of a customer or other third party.

Where the records referred are kept by a Regulated Entity outside the IFSC, the Regulated Entity shall:

a) take all reasonable steps to ensure that the records are kept in a manner consistent with the Guidelines;
b) ensure that the records are easily accessible to it; and
c) ensure that the records are immediately made available for inspection, when so desired by the Authority.

Further all Regulated Entities shall:

a) verify if there are secrecy or data protection laws that would restrict access without delay to the records referred by the Regulated Entities, the Authority or the law enforcement agencies of India; and
b) where such law exists, obtain without delay, the certified copies of the relevant records and keep such copies in a jurisdiction which allows access by those persons referred above.

Sample Questions

1. Which of the following is correct about the duty of a Regulated Entity?
   a) Every member of Regulated Entity's Senior Management shall be responsible for the Regulated Entity's compliance under IFSCA (AML, CFT and KYC) Guidelines
   b) Only Compliance officer shall be responsible for the Regulated Entity's compliance under IFSCA (AML, CFT and KYC) Guidelines
   c) Only Designated Director shall be responsible for the Regulated Entity's compliance under IFSCA (AML, CFT and KYC) Guidelines
   d) Only Principal Officer shall be responsible for the Regulated Entity's compliance under IFSCA (AML, CFT and KYC) Guidelines

2. While implementing Risk Based Approach, a Regulated Entity must ensure which of the following?
   a) The RBA is objective and proportionate to the risks
   b) The RBA is based on reasonable grounds
   c) The RBA is reviewed and updated at appropriate intervals
   d) All of the above

3. Which of the following is not true about Customer Due Diligence process?
   a) Identifying the customer and verifying that customer's identity
   b) **Not obtaining information on the purpose and intended nature of the business relationship.**
   c) Conducting ongoing due diligence on the business relationship and scrutiny of transactions
   d) Knowing customer's business and risk profile, including, where necessary, the source of funds too.

4. Obtaining the approval of Senior Management to commence or continue the business relationship with a client is a measure specified under which process?
   a) Client Risk Categorisation
   b) Simplified Customer Due Diligence
   c) Enhanced Due Diligence
   d) All of the above

Chapter-6 IFSCA Guidelines for KYC Norms

Learning Objective- After studying this chapter, you should know about:

- The IFSCA KYC guidelines and process to be followed by every Regulated Entity from the client at the time of commencement of an account-based relationship.

6.1 IFSCA guidelines for KYC norms

The provisions of IFSCA (AML, CFT and KYC) Guidelines apply to every Regulated Entity falling under the purview of IFSCA. The provisions of these Guidelines also apply to a Financial Group[35] of the Regulated Entity, to specified extent.[36]

The Chapter4 – 'Customer Risk Management' of the IFSCA (AML, CFT and KYC) Guidelines deals with assessing the risk posed by a prospective client to the Registered Intermediaries.

Risks identified while assessing the business risks shall be used for the customer risk assessment. The customer risk assessment shall be performed while taking into consideration the parameters, or the process as specified below. The outcome of the Customer risk assessment shall be used to assign the risk rating of the customer as high, medium or low, proportionate to the ML/TF risks.

6.1.1 Assessing customer AML risks

(a) A Regulated Entity shall:

i. undertake a risk-based assessment of every customer; and

ii. assign the customer a risk rating proportionate to the ML/TF risks.

(b) The customer risk assessment referred to in Clause (a) above, shall be completed prior to undertaking Customer Due Diligence for new customers, and also where the Regulated Entity otherwise feels necessary, for existing customers.

(c) When undertaking an assessment under Clause 4.1 (a) (i) above, a Regulated Entity shall:

i. identify the customer and Beneficial Owner, if any;

ii. obtain information on the purpose and intended nature of the business relationship;

[35]"Financial Group" means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.

[36]https://ifsca.gov.in/Legal/Index/TCce8MyOmco=

iii. obtain information on, and take into consideration, the nature of the customer's business;
iv. take into consideration the nature of the customer, its ownership, control structure, and its Beneficial Ownership, wherever applicable;
v. take into consideration the nature of the customer's business relationship with the Regulated Entity;
vi. take into consideration the customer's country of origin, residence, nationality, place of incorporation or place of business;
vii. take into consideration the relevant product, service or transaction; and,
viii. take into consideration the beneficiary of the policy including any Beneficial Owner of such beneficiary, if it is providing the customer with a life insurance or other similar policy.

The risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off.

6.1.2 Factors that may indicate high ML/TF risk

When assessing if there is a high risk of ML/TF in a particular situation, a Regulated Entity shall take into account, among other things:

(a) Customer risk

i. Whether the customers are from high-risk businesses / activities / sectors, as well as from other sectors as may be identified by it;
ii. Whether the ownership structure of the legal person or arrangement appears unusual or excessively complex;
iii. Whether the business relations are conducted under unusual circumstances (e.g., significant unexplained geographic distance between the Regulated Entity and the customer);
iv. Whether the companies have nominee shareholders or shares in bearer form;
v. Whether the legal persons or legal arrangements are personal asset holding vehicles; and,
vi. Whether the corporate structure of the customer is unusual or excessively complex given the nature of the business.

(b) Country or Geographic risk

i. Whether the countries or jurisdictions the Regulated Entity is exposed to, either through its own activities (including where its branches and subsidiaries operate in) or the activities of its customers (including the Regulated Entity's network of correspondent account relationships) have relatively high levels of corruption, organized crime or inadequate AML/CFT measures, as identified by the FATF;

ii. Whether the countries or jurisdictions are identified by any credible body as having significant levels of corruption, terrorism financing or other criminal activities;
iii. Whether the countries or jurisdictions are identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems;
iv. Whether the countries or jurisdictions do not have effective systems to counter ML/TF; or not implementing the AML/CFT measures that are consistent with FATF Recommendations;
v. Whether the countries or jurisdictions are subject to sanctions, embargos or similar measures issued by International Organisations or India;
vi. Whether the countries or jurisdictions are funding or supporting the terrorism; and,
vii. Whether countries or jurisdictions have organizations operating within their territory that have been designated by India, other countries or International Organizations as terrorist organizations.

(c) product, service, transaction or delivery channel risk factors

i. Whether the service involves private banking;
ii. Whether the product, service or transaction is one that might favour anonymity;
iii. Whether the situation involves non-face-to-face business relationships or transactions, without adequate safeguards;
iv. Whether the payments received are from unknown or unassociated third parties;
v. Whether the services offered are in relation to nominee directors, nominee shareholders or the formation of companies in another country; and
vi. Whether there are anonymous transactions or any transaction which involves frequent payments, received from unknown or unassociated third parties.

When assessing the risk factors, the Regulated Entity shall examine the overall risk while keeping in mind that the presence of one or more risk factors alone may not always indicate a high risk of ML/TF in a particular situation.

6.1.3 Factors that may indicate low ML/TF risks

When assessing if there is a low risk of ML/TF in a particular situation, a Regulated Entity shall take into account, among other things:

(a) customer risk factors, including whether the customer is:

i. a Government entity;

ii. public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.
iii. regulated financial institution incorporated or established outside India that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.
iv. a subsidiary of a regulated financial institution referred to in sub-clause (iii) above, if the law that applies to the Parent entity ensures that the subsidiary also observes the same AML standards as that of its Parent entity.
v. a public body or a publicly owned enterprise.
vi. a resident established or registered in a geographical area of low risk.

(b) product, service, transaction or delivery channel risk factors, including whether the product or service is:

i. a Contract of Insurance that is non-life insurance;
ii. a Contract of Insurance that is a life insurance product with no investment return or redemption or surrender value;
iii. an insurance policy for a pension scheme that does not provide for an early surrender option and cannot be used as collateral;
iv. a Contract of Insurance which is a reinsurance contract that is ceded by an insurer which is a regulated financial institution;
v. a pension, superannuation or similar scheme that satisfies the following conditions:
   (aa) the scheme provides retirement benefits to employees;
   (bb) contributions to the scheme are made by way of deductions from wages; and
   (cc) the scheme rules do not permit the assignment of a member's interest.

vi. a product where the ML/TF risks are adequately managed by other factors such as transaction limits or transparency of ownership; and
vii. financial products or services that provide appropriately defined and limited services to certain types of customers (e.g., to increase customer access for financial inclusion purposes).

When assessing the risk factors, the Regulated Entity shall examine the overall risk while keeping in mind that the presence of one or more risk factors alone may not always indicate a low risk of ML/TF in a particular situation.

6.1.4 Business relationship should not be established in the following cases:

The Regulated Entity shall not establish the business relationship with the customer, which is a legal person or legal arrangement, in the following cases: -

(a) where the ownership or control arrangements of the customer prevent the Regulated Entity from identifying one or more of the customer's Beneficial Owners;
(b) where there are anonymous accounts, accounts in fictitious names, or a nominee account which is held in the name of one person, but is controlled by or held for the benefit of another person whose identity has not been disclosed to the Regulated Entity; or
(c) a Shell Financial Institution.

6.2 Customer Due Diligence Process

6.2.1Customer Due Diligence

Chapter V of the IFSCA (AML, CFT and KYC) Guideline elucidates the requirements for carrying out customer due diligence by a regulated entity. As per these guidelines, a Customer or Client means a person who is engaged in a financial transaction or activity with a Regulated Entity and includes a person on whose behalf the person engaged in the transaction or activity, is acting.

A Regulated Entity after assigning risk rating for each Customer proportionate to their AML/CFT risks, shall undertake the Customer Due Diligence. While undertaking the CDD, a Regulated Entity shall: -

i. undertake Customer Due Diligence measures as detailed under Clause 5.4, in respect of all the customers;
ii. undertake Enhanced Customer Due Diligence measures as detailed under Clause 5.6, in addition to the CDD measures detailed under Clause 5.4, in respect of the customer who has been assigned 'high risk'; and
iii. undertake Simplified Customer Due Diligence measures as detailed under Clause 5.7 by modifying Customer Due Diligence process detailed under Clause 5.4, in respect of a customer who has been assigned 'low risk'.

6.2.2 Timing of CDD

a) Except as otherwise provided in Clause 5.3 and 5.4, a Regulated Entity shall undertake the Customer Due Diligence of a customer: -
    i. at the time of establishing business relationship, as mandated under Clause 5.4.1 (a) to (c); and
    ii. after establishing a business relationship, as mandated under Clause 5.4.1.(d).

b) A Regulated Entity shall also undertake Customer Due Diligence if, at any time:
    i. in relation to an existing customer, it doubts the veracity or adequacy of documents, data or information obtained for the purposes of Customer Due Diligence;
    ii. it suspects ML/TF; or

iii. there is a change in risk-rating of the customer, or it is otherwise warranted by a material change in circumstances of the customer.

6.2.3 Establishing business relationship before verification

(a) A Regulated Entity may establish a business relationship with a customer before completing the verification required under Clause 5.4.1, subject to fulfilling the following conditions:

i. the deferral of completion of the verification of the customer or Beneficial Owner is essential in order not to interrupt the normal conduct of a business relationship;
ii. there is low risk of occurrence of ML/TF activity and any such risks identified can be effectively managed by the Regulated Entity;
iii. in relation to a bank account opening, there are adequate safeguards in place to ensure that the account is not closed, and transactions are not carried out by or on behalf of the account holder (including any payment from the account to the account holder) before verification has been completed; and
iv. subject to Clause 5.3 (b) below, the relevant verification is completed as soon as reasonably practicable and, in any event, it should not exceed 30 business days after the establishment of business relationship.

(b) Where a Regulated Entity is not able to comply with the 30-day requirement, it shall, prior to the end of the 30-day period:

i. document the reason for its non-compliance;
ii. complete the verification as soon as possible; and
iii. record the non-compliance event for reporting to its Governing Body[37].

(c) The Regulated Entity shall suspend business relationship with the customer and refrain from carrying out further transactions (except to return funds to their sources, to the extent that is possible) if such verification remains uncompleted for 30 days after the establishment of business relationship.

(d) The Regulated Entity shall terminate business relations with the customer if such verification remains uncompleted for 120 days after the establishment of business relationship.

(e) A Regulated Entity shall ensure that its AML/CFT systems and controls referred to in Clause 3.3 above, include internal risk management policies and procedures concerning the conditions under which such business relationships may be established with a customer

[37]The meaning of a governing is provided in clause 1.3.20 of the IFSCA AML, CFT and KYC Guidelines: https://ifsca.gov.in/CommonDirect/GetFileView?id=38fea9cc5969551d78bf00e670f64da8&fileName=Approved_Master_Guidelines__1__20260105_0719.pdf&TitleName=Legal

before completing verification and should also factor the above time limitation in its policies, procedures and controls.

6.3 Customer Due Diligence Requirements

6.3.1 Undertaking Customer Due Diligence (CDD)

In undertaking Customer Due Diligence as required under Clause 5.1.(a) of the IFSCA (AML, CFT and KYC) Guidelines, the following measures shall be undertaken by a Regulated Entity:

a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.
b) Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, in such a manner that the Regulated Entity is satisfied that it knows who the beneficial owner is. Similarly, for legal persons and arrangements, the CDD shall include Regulated Entity taking reasonable steps to understand the nature of the customer's business, its ownership and control structure.
c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.
d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of business relationship to ensure that the transactions that are being conducted, are consistent with the Regulated Entity's knowledge of the customer, customer's business and risk profile, including, where necessary, the source of funds.

6.3.2 Identification of Customer

a) If a customer is a natural person, a Regulated Entity shall obtain at least the following information:
   i. Full name, including any aliases;
   ii. Unique Identification Number (such as an Identity card number, passport number, etc.);
   iii. Date of birth;
   iv. Nationality;
   v. Legal domicile;
   vi. Current residential address; (other than a post office box address);
   vii. Contact details such as personal, office or work telephone numbers.

b) If a customer is a legal person or legal arrangement, a Regulated Entity shall obtain at least the following information:
   i. The full name and any trading name;

ii. Unique identification Number (i.e., Tax identification number or equivalent where this exists, incorporation number or business registration number);
iii. Registered or business address, and if different, its principal place of business;
iv. Date of establishment, incorporation or registration;
v. Place of incorporation or registration.

c) Further, in cases where the customer is a legal person or legal arrangement, a Regulated Entity shall, also identify the legal form, constitution and powers that regulate and bind the legal person or legal arrangement. In addition to this, Regulated Entity shall also identify and screen the related parties or connected parties of such customer and should remain apprised of any changes to connected parties. For identification of the connected parties, a Regulated Entity shall obtain at least the following information of each related or connected party:
   i. full name, including any aliases; and
   ii. Unique Identification Number (such as an Identity card number, passport number, etc.).

6.3.3 Verification of Identity of Customer

a) A Regulated Entity shall verify the identity of the customer using reliable, independent source data, documents or information. Where the customer is a legal person or legal arrangement, a Regulated Entity shall verify the legal form, proof of existence, constitution and powers that regulate and bind the customer, using reliable, independent source data, documents or information.
b) When relying on documents, a Regulated Entity should be aware that the most reliable documents to verify the identity of the customer are those which are most difficult to obtain illegally or to counterfeit. These may include government-issued identity cards or current valid passport, reports from independent company registries, published or audited annual reports and other reliable sources of information. The rigor of the verification process should be commensurate with the customer’s risk profile.
c) In verifying the identity of a customer, a Regulated Entity may obtain the following documents:

6.3.3.1 In case of Natural Persons

(i) any of the OVD specified under these Guidelines that contains photograph of the customer, name, unique identification number, date of birth and nationality; and
(ii) residential address based on OVD or recent utility bill, bank statement or such other documents specified under the definition of OVD.

6.3.3.2 In case of Legal persons or Legal Arrangements

(i) Name, legal form, proof of existence and constitution: - the verification for the same can be obtained from certificate of incorporation, certificate of good standing, partnership deed/agreement, trust deed, constitutional document, certificate of registration or any other document from a reliable independent source; and

(ii) Powers that regulate and bind the legal person or legal arrangement: - This can be ascertained from the constitutional documents, as well as the names of the relevant persons having a Senior Management position in the legal person or legal arrangement and board resolution or similar document authorising the opening of an account and appointment of its authorised signatories.

6.3.3.3 V-CIP Process for Onboarding Indian Nationals

Video based Customer Identification Process" or "V-CIP" means an alternate method of customer identification with facial recognition and customer due diligence, by an authorised official of the Regulated Entity, by undertaking seamless, secure, live, informed & consent based audio-visual interaction with the customer to obtain identification information required for Customer Due Diligence purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process.[38]

The Regulated Entities may undertake V-CIP to carry out:

(a) CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of customers which are non-natural persons.

(b) Updation/Periodic updation of KYC for eligible customers.

Further, the Regulated Entities opting to undertake V-CIP, shall adhere to the minimum standards and procedure as specified in the Annexure II, clauses 1.2 and 1.3 respectively of the IFSCA (AML, CTF and KYC) Guidelines.

6.3.3.4 Digital KYC Process for Indian Nationals

For undertaking CDD of Indian nationals, the Regulated Entities shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

[38] Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face customer identification procedure for the purpose of these Guidelines.

(a) the Aadhaar number where the customer decides to submit his Aadhaar number voluntarily to a bank or any Regulated Entity notified under first proviso to sub-section (1) of section 11A of the Act; or

(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or

(bb) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document[39] thereof containing the details of the customer's identity and address; and

(b) the Permanent Account Number or the equivalent e-document thereof, as defined in Income-tax Rules, 1962; and

(c) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof, as may be required by the Regulated Entity, considering all the conditions as specified by IFSCA from time to time.

6.3.4 Identification and Verification of Identity of Natural Person appointed to act on behalf of Customer

a) Where a customer is a natural person or legal person, or legal arrangement to act on its behalf for establishing business relations with a Regulated Entity, the Regulated Entity shall identify each natural person who acts or is appointed to act on behalf of such natural or legal person 20 or legal arrangement by obtaining information as specified in Clause 5.4.2 of the guidelines (i.e., identification of customer).
Provided that in case of a trust, the Regulated Entity shall ensure that trustees disclose their status at the time of commencement of a business relationship or when carrying out transactions as specified in clause (b) of sub-rule (1) rule 9 of the Rules.

b) Further, the Regulated Entity shall verify the identity of each such natural persons using reliable, independent source data, documents or information. Furthermore, the Regulated Entity shall verify the authorisation of each natural person appointed to act on behalf of the customer by obtaining at least the following:
   i. The appropriate documentary evidence authorising the appointment of such natural person by the customer to act on his or its behalf which may include power of attorney, resolution passed by Governing Body or authorisation granted to transact on its behalf.

[39]As per IFSCA AML, CFT and KYC Guideline, "Equivalent e-document" means an electronic equivalent of a document, issued by the issuing authority of such document with its valid Digital Signature, including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016 or its equivalent in other jurisdictions, as may be recognised by the Authority.

ii. Where there is a long list of natural persons appointed to act on behalf of the customer (e.g., a list comprising more than 10 authorized signatories), the Regulated Entity shall verify those natural persons who will deal directly with the Regulated Entity.

6.3.5 Identification and Verification of Identity of Beneficial Owners

Where there is one or more Beneficial Owners in relation to a customer, the Regulated Entity shall identify the Beneficial Owners and take reasonable measures to verify their identities using the relevant information or data obtained from reliable, independent sources.

For the identification and verification of Identity of Beneficial Owner, the Regulated Entity should consider the following in relation to:

(a) Customers that are legal persons

i. The identity of the natural person(s) (whether acting alone or together) exercising control over the legal person through ownership or who ultimately owns the legal person;
ii. To the extent that there is doubt as to whether the natural persons who ultimately own the legal person are the beneficial owners or where no natural persons ultimately own the legal person, identify the natural person(s) (if any) who ultimately control the legal person or have ultimate effective control over the legal person.

(b) Customers that are legal arrangements

i. Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen per cent. or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.
ii. In all other types of legal arrangements, the Regulated Entity shall identify persons in equivalent or similar positions.

6.3.6 Parameters to Identify and Verify the Identity of Beneficial Owners

a) Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means. Explanation- For the purpose of this sub-clause-
   i. "Controlling ownership interest" means ownership of or entitlement to more than ten per cent. of the shares or capital or profits of the company;
   ii. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

b) Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than ten per cent of capital or profits of the partnership or who exercises control through other means.

Explanation - For the purpose of this clause, "Control" shall include the right to control the management or policy decision;

c) Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of or entitlement to more than fifteen per cent. of the property or capital or profits of the unincorporated association or body of individuals.[40]

d) Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with ten per cent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

Explanation: - For the purpose of determination of beneficial owner, any amendment made under sub-rule 3 of rule 9 of Rules, shall be applicable in addition to the requirements under these Guidelines.

e) As per rule 9(3)(f) of the Rules, unless the Regulated Entity has doubts about the veracity of the CDD information, or suspects that customer may be connected with ML/TF, it shall not be required to identify and verify the identity of any shareholder or beneficial owner of a customer in the following –

f) Where the client or the owner of the controlling interest is an entity listed on the stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary of such listed entities and such other entities who have been excluded from the requirements regarding identifying and verifying beneficial owners of a customer under the Act and Rules.

g) As per the second proviso of rule 9(1)(c) of the Rules, in cases where a customer is subscribing or dealing with depository receipts or equity shares issued or listed in jurisdictions notified by the Central Government, of a company incorporated in India, and it is acting on behalf of a beneficial owner who is resident of such jurisdiction, the

[40]Explanation: The term 'body of individuals' includes societies. Where no natural person is identified under (a) to (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

determination, identification and verification of such beneficial owner, shall be as per the norms of such jurisdiction and nothing in sub-rules (3) to (9) of the rule 9 of the Rules shall be applicable for due-diligence of such beneficial owner.

6.3.7 Identifying and verifying beneficiary of a life insurance policy

For life or other investment-related insurance business, Regulated Entity shall, in addition to the CDD measures required for the customer and the beneficial owner, conduct the following CDD measures on the beneficiary(ies) of life insurance and other investment related insurance policies, as soon as the beneficiary(ies) are identified/designated:

(i) A Regulated Entity shall, as soon as a beneficiary of a life policy is identified as a specifically named natural person, legal person or legal arrangement, obtain the full name, including any aliases, of such beneficiary;

(ii) For beneficiary(ies) that are designated by characteristics or by class (e.g., spouse or children at the time that the insured event occurs) or by other means (e.g., under a will) – the Regulated Entity shall obtain sufficient information concerning the beneficiary(ies) to satisfy itself that it will be able to establish the identity of the beneficiary(ies) at the time of the payout.

(iii) In relation to life insurance policies, the Regulated Entity should be required to take reasonable measures to determine whether the beneficiaries and/or, where required, the beneficial owner of the beneficiary, are PEPs. This should occur, at the latest, at the time of the payout. Where higher risks are identified, financial institutions should be required to inform Senior Management before the payout of the policy proceeds, to conduct enhanced scrutiny on the whole business relationship with the policyholder, and to consider making a Suspicious Transaction Report.

6.3.8 Information on the Purpose and Intended Nature of Business Relations

(a) A Regulated Entity shall, while establishing business relationship, understand and as appropriate, obtain information from the customer as to the purpose and intended nature of business relations.

(b) The measures taken by a Regulated Entity to understand the purpose and intended nature of business relations should be commensurate with the risk profile and complexity of the customer's business.

6.4 Accounts of Politically Exposed Persons

(a) A Regulated Entity shall implement appropriate internal risk management systems, policies and procedures to determine if a customer or any natural person appointed to act on behalf of the customer, or any beneficial owner of the customer is a politically exposed person

(PEP) or in case of a life insurance or other similar policy, if a beneficiary of the policy, or a Beneficial Owner of a beneficiary, is a PEP.

(b) A Regulated Entity shall, in addition to undertaking CDD measures, undertake at least the following additional measures where a customer or any beneficial owner of the customer or beneficiary of a life insurance or other similar policy, or a Beneficial Owner of a beneficiary is determined by the Regulated Entity to be a PEP:

i. Collect by appropriate and reasonable means, adequate information including information about the source of wealth and income of family members, any beneficial owner and close relatives;
ii. Verify the identity before accepting the PEP as a customer;
iii. Obtain approval from its Senior Management before opening an account of a PEP or making any payout under the life insurance or other similar policy to the PEP;
iv. In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, obtain the Senior Management's approval to continue the business relationship;
v. Increase the degree and nature of ongoing monitoring of the business relationship, to determine whether the customer's transactions or activities appear unusual or suspicious.
vi. Carry out the additional Customer Due Diligence for circumstances specified in sub-clauses (i) to (v) above, before making any payout under the life insurance or other similar policy.

(c) A Regulated Entity may adopt a risk-based approach in determining whether to perform enhanced CDD measures or the extent of enhanced CDD measures to be performed for: -

i. PEP, their family members and close associates;
ii. International Organisation PEP, their family members, and close associates;
iii. PEP who has stepped down from their prominent public functions, taking into consideration the level of influence such persons may continue to exercise after stepping down, their family members and close associates, except in cases where their business relations or transactions with the Regulated Entity present a high risk for ML/TF.

6.5 Enhanced Due Diligence

(a) Where the risks of ML/TF are high, a Regulated Entity shall conduct enhanced CDD measures, consistent with the risks identified. The enhanced CDD measures are as follows: -

i. Obtaining additional information on the customer (e.g., occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.

ii. Obtaining information and taking additional steps to examine the ownership and financial position, including source of wealth and source of funds of the customer or, if applicable, of the Beneficial Owner.
iii. Obtaining information and taking additional steps to record the purpose behind conducting the specified transaction and the intended nature of the relationship between the transaction parties.
iv. Obtaining the approval of Senior Management to commence or continue the business relationship.
v. Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination; and,
vi. Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

(b) Where applicable, it is required that first payment made by a customer in order to open an account with a Regulated Entity shall be carried out through a bank account in the customer's name with:
   i. a Bank;
   ii. a regulated financial institution whose entire operations are subject to regulation and supervision, including AML/CFT regulation and supervision, in a jurisdiction where its regulations on AML/CFT are equivalent to the standards set out in the FATF recommendations; or
   iii. a subsidiary of a regulated financial institution referred to in (ii), if the law that applies to the Parent entity ensures that the subsidiary also observes the same AML/CFT standards as its Parent entity.

The Regulated Entities shall specifically apply enhanced due diligence measures, proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

6.6 Simplified Customer Due Diligence

(a) Where the risks of ML/TF are low, a Regulated Entity may conduct simplified CDD measures, which should be commensurate with the low risk factors. Examples of possible measures are:

i. Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship as specified under Clause 5.3.
ii. Reducing the frequency of customer identification updates.
iii. Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

iv. Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship but inferring the purpose and nature from the type of transactions or business relationship established.

(b) Simplified CDD (SCDD) measures shall not be conducted where there is a suspicion of ML/TF.

6.7 Ongoing customer due diligence

While undertaking the ongoing customer due diligence, as required under Clause 5.4.1.(d), the following requirements shall be complied with by a Regulated Entity: -

i. The Regulated Entity shall monitor its business relations with the customer on an ongoing basis.
ii. The Regulated Entity during the course of business relations with a customer, shall observe the conduct of the customer’s account and scrutinize transactions undertaken throughout the course of business relations, to ensure that the transactions are consistent with Regulated Entity’s knowledge of the customer, its business and risk profile and where appropriate, may seek the source of wealth and source of funds.
iii. The Regulated Entity shall pay particular attention to any complex, unusually large or unusual patterns of transactions undertaken throughout the course of business relations, that have no apparent or visible economic or legitimate purpose.
iv. The Regulated Entity shall make further enquiries into the background and purpose of the transaction specified in sub-clause (iii) above and document its findings so that this information is made available to the relevant authorities, should the need arise.
v. A Regulated Entity shall periodically review each customer to ensure that the risk rating assigned under Clause 4.1. (a) (ii) above, is commensurate with the ML/TF risks posed by the customer.
vi. Where there are indications that the risks associated with an existing business relation with the customer may have increased, the Regulated Entity shall request additional information and conduct a review of the customer’s risk profile in order to determine if additional measures are necessary.
vii. The Regulated Entity shall ensure that the Customer Due Diligence data, documents and information obtained in respect of customers, natural persons appointed to act on behalf of the customers, related parties of the customers and beneficial owners of the customers, are relevant and kept up-to-date by undertaking the review of adequacy of the existing Customer Due Diligence data, documents and information, particularly for customers with high-risk rating.

6.8 Ongoing sanctions screening

A Regulated Entity shall review its customers, their business and transactions against United Nations Security Council sanctions lists and also against any other relevant sanctions list when complying with Clause 5.4.1 (d).

6.9 Failure of Regulated Entity to conduct or complete customer due diligence

(a) In cases where a Regulated Entity is unable to conduct or complete the requisite Customer Due Diligence for a customer in accordance with Clause 5.4.1, it, to the extent relevant, shall:

i. not open an account or otherwise provide a service;
ii. not carry out a transaction with or for the customer;
iii. not otherwise establish a business relationship;
iv. terminate or suspend any existing business relationship with the customer;
v. return any monies or assets received from the customer; and,
vi. consider whether the failure to conduct or complete Customer Due Diligence necessitates the filing of a Suspicious Transaction Report (STR).

Provided that no application for onboarding or periodic updation of KYC shall be rejected, in case of Persons with Disabilities (PwDs), without application of mind. Reason(s) of rejection shall be duly recorded by the officer concerned.

(b) A Regulated Entity is not bound to comply with sub-clauses (a) (i) to (v) above, if it amounts to “tipping off” of the customer, or FIU-IND directs the Regulated Entity to act otherwise.

6.10 Periodic Updation

A Regulated Entity shall adopt a risk-based approach for periodic updation of CDD. The periodicity of updation from the date of opening of the account / last CDD updation for different categories of customers is as follows: -

i. Annually- for high-risk customers;
ii. once in three years- for medium risk customer; and,
iii. once in every five years- for low-risk customers.

Provided that the periodicity of such updation in case of resident Indian customer having an existing client relationship with the Financial Group in India, shall be as follows:

(a) once in every two years - for high-risk customers,

(b)once in every eight years - for medium risk customers and

(c) once in every ten years - for low-risk customers.

Provided further that where the risk categorization made by the Financial Group entity differs from the risk categorization made by the Regulated Entity, the stricter of the two periodicity shall apply.

Policy in this regard shall be documented as part of Regulated Entity's internal KYC policy, which is duly approved by the Governing Body of the Regulated Entity.

(a) Individual Customers:

i. No change in CDD information:

In case of no change in the CDD information, a self-declaration from the customer in this regard may be obtained through mobile number registered with the Regulated Entity or through digital channels (such as online banking / internet banking, e-mail or mobile application of Regulated Entity).

ii. Change in address:

(aa) In case of a change only in the address details of the customer, a self-declaration of the new address may be obtained from the customer through customer's email-id registered with the Regulated Entity, customer's mobile number registered with the Regulated Entity, digital channels (such as online banking internet banking, e-mail or mobile application of the Regulated Entity). The declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

(bb) Further, a Regulated Entity shall obtain a copy of OVD or the equivalent e-documents thereof for the purpose of proof of address declared by the customer at the time of periodic updation. Such requirement, however, shall be clearly specified by the Regulated Entity in its internal KYC policy, duly approved by its Governing Body.

(b) Customers other than Natural Persons:

i. No change in CDD information:

In case of no change in the CDD information of a customer, which is a non-natural person, a self-declaration through email id registered with the Regulated Entity, digital channels (such as online banking / internet banking, mobile application of Regulated Entity), a letter duly signed by authorised official and requisite resolutions in this regard shall be obtained from the customer. Further, a Regulated Entity shall ensure that Beneficial Ownership (BO) information available with them is accurate and up to-date.

ii. Change in CDD information:
   In case of change in CDD information, Regulated Entity shall undertake fresh CDD process as is applicable for on boarding a new customer which is a non-natural person.

(c) Additional measures:

In addition to the above, a Regulated Entity shall ensure that:

i. The KYC documents of the customer as per the current CDD standards are available with it. This is applicable even if there is no change in customer information but the documents available with the Regulated Entity are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the Regulated Entity has expired at the time of periodic updation of CDD, Regulated Entity shall undertake fresh CDD process equivalent to that applicable for on boarding a new customer.
ii. In case of Indian National, the customer's PAN details, if available with the Regulated Entity, is verified from the database of the issuing authority at the time of periodic updation of CDD.
iii. Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, the Regulated Entity shall ensure that the information / documents obtained from the customers at the time of periodic updation of CDD are promptly updated in its records / database and an intimation, mentioning the date of updation of CDD details, is provided to the customer.
iv. In order to ensure customer convenience, a Regulated Entity may consider making available the facility of periodic updation of CDD at any of its branch, or in such other facilities in terms of its internal KYC policy, duly approved by its Governing Body.
v. A Regulated Entity shall adopt a risk-based approach with respect to periodic updation of CDD. Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the Regulated Entity (such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of CDD only where account is maintained, a more frequent periodicity of CDD updation than the minimum specified periodicity etc.), shall be clearly specified in its approved internal KYC policy.
vi. A Regulated Entity shall ensure that its internal KYC policy and processes on updation / periodic updation of CDD are transparent and adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements.
vii. In case of any update in the documents submitted by the customer at the time of establishment of business relationship and thereafter, as necessary; customers shall

submit to the Regulated Entity the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at Regulated Entity's end.

With effective implementation of IFSCA guidelines for KYC norms in International Financial Service Centres by Regulated Entities, IFSCA's crucial role in maintaining market integrity, investor confidence, and the orderly functioning of India's International Financial Markets can be duly and efficiently achieved.

6.11 Differences between IFSCA AML/CFT guidelines and other Indian regulators

IFSCA Guidelines	Other Indian Regulators
IFSCA guidelines are tailored to the unique global nature of IFSC operations	The fundamental goals of Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) are shared across all Indian regulators (like RBI, SEBI, IRDAI, PFRDA)
IFSCA acts as a single point of regulation for diverse financial activities within IFSC	Other Indian regulators focus on specific sectors like banking, securities, insurance, or pensions
Given the international focus of IFSCA, its AML/CFT guidelines align closely with the recommendations of the Financial Action Task Force (FATF), the global standard-setter for combating illicit financial flows	The AML/CFT guidelines of Indian Regulators are more aligned with Indian Financial Environment
IFSC entities primarily deal with international clients and cross-border transactions, requiring a strong emphasis on global KYC, CDD, and sanctions screening procedures aligned with international practices	The Indian Regulators primarily deal with domestic clients, requiring a strong alignment with Indian laws, rules and regulations
IFSCA aims to provide a world-class regulatory environment with ease of doing business, which may lead to streamlined KYC procedures potentially differing from those for domestic entities	The KYC/CDD process being followed by other Indian Regulators have been carved out in such a manner so as to suit the Indian business requirements

Sample Questions

1. While performing customer risk assessment, which factor/s will a regulated entity ensure?
   a) Identify the customer and Beneficial Owner
   b) Obtain information on the purpose and intended nature of the business relationship
   c) Both of the above
   d) None of the above

2. Where the ownership or control arrangements of the customer prevent the Regulated Entity from identifying one or more of the customer's Beneficial Owners, the Regulated Entity shall not establish the business relationship with the customer. State True or False.
   a) TRUE
   b) FALSE

3. Under which of the following circumstances, a Regulated entity must perform Enhanced Due Diligence?
   a) PEP, their family members and close associates
   b) Where the risks of ML/TF are high
   c) PEP who has stepped down from their prominent public functions
   d) All of the above

4. Which of the following is true about IFSCA AML/CFT Guidelines?
   a) These guidelines are more aligned with Indian Financial Environment
   b) These guidelines have been carved out in such a manner so as to suit the Indian business requirements
   c) These guidelines deal with domestic clients, requiring a strong alignment with Indian laws, rules and regulations
   d) These guidelines are tailored to the unique global nature of IFSC operations

Chapter-7 Discussion on PMLA related Cases

Learning Objective: After studying this chapter, you should know about:

- Practical implementation and coverage of PMLA through case studies.

This Chapter covers different cases based on FIU-IND and IFSCA Adjudicating Orders in the scope of Prevention of Money Laundering Act (PMLA). They are described in the following manner:

7.1 FIU-IND V/S Bybit Fintech Limited (Bybit), a Virtual Digital Asset Service Provider

Facts of the Case-

The Financial Intelligence Unit-India (FIU-IND) in furtherance of the powers conferred upon the Director FIU-IND under Section 13(2)(d) of the Prevention of Money Laundering Act, 2002 (as amended) ("PMLA") has imposed a monetary penalty of Total ₹9,27,00,000 (Nine crore twenty-seven lakh rupees) on Bybit Fintech Limited (Bybit) a Virtual Digital Asset Service Provider (VDA SP) with reference to the violations of its obligations under the PMLA read with the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 ("PML Rules") issued thereunder and applicable guidelines and advisories issued by the Director FIU-IND.

Findings of the case

As a Virtual Digital Asset Service Provider (VDA SP), Bybit is classified as a 'reporting entity' under Section 2(1) (wa) of the Prevention of Money Laundering Act (PMLA). Bybit kept expanding its services in the Indian market without securing mandatory registration with the FIU-IND. The persistent and continuous non-compliance caused FIU-IND to block their websites to stop operations under the Information Technology Act, 2000 through the Ministry of Electronics and Communication Technology (MEITY).

It is noteworthy that FIU-IND had previously issued comprehensive Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) Guidelines for Reporting Entities offering Services related to Virtual Digital Assets on March 10, 2023. Furthermore, a detailed circular regarding the registration of Virtual Digital Asset Service Providers as reporting entities was issued on October 17, 2023.

Order: -

After conducting a thorough examination of both written and oral submissions from Bybit, the Director of FIU-IND found Bybit liable of the charges for various violations. In an order dated

January 31st, 2025, and exercising authority under Section 13 of the PMLA, it was unequivocally established that Bybit was in violation of Section 12(1) of the PMLA read with Rule 2(1)(h), Rule 7(2), Rule 8(2) Rule 8 (4), Rule 3(1)(D) and Rule 7(3) of PMLR, 2005. Consequently, a total penalty of Rs. 9,27,00,000 was imposed on Bybit.[41]

7.2 IFSCA V/S Prowess Insurance Brokers Pvt. Ltd. (PIBPL)

Facts of the Case

M/s Prowess Insurance Brokers Pvt. Ltd ("PIBPL" or "Noticee") is registered with Insurance Regulatory and Development Authority of India ("IRDAI"), as 'Direct Broker (Life & General)'. IRDAI granted renewal of certificate of registration (CoR) to PIBPL which was valid from September 22, 2018, till September 21, 2021.

The IRDAI in terms of IRDAI (IFSC Insurance Intermediary Offices) Guidelines, 2019 (hereinafter after referred to as 'IRDAI IIIO Guidelines, 2019') had granted approval/authorization dated August 17,2020 to PIBPL to open branch in GIFT IFSC and operate as IFSC Insurance Intermediary Office (IIIO).

As per clause 11 of the said IRDAI guidelines, validity of approval/authorization granted to the IIIO by IRDAI was for a period co-terminus with the expiry of the original CoR issued by the IRDAI to PIBPL. Accordingly, the CoR for the Noticee was issued on September 22, 2018, and was valid till September 21, 2021.

The IFSCA notified IFSCA (Insurance Intermediary) Regulations, 2021 (hereinafter referred to as IIIO Regulations, 2021) which superseded the IRDAI IIIO Guidelines, 2019. Under the IIIO Regulations, 2021, PIBPL was expected to seek and obtain renewal of its CoR beyond September 21, 2021 from IRDAI, and subsequently required to file an application with IFSCA for CoR for its Branch office at GIFT-IFSC, as the authorization/approval for the IFSC branch office of PIBPL was also valid till September 2021 only.

The Noticee/Branch office of PIBPL in GIFT IFSC had informed the IFSCA on January 6, 2022 that their application for renewal of registration is pending with IRDAI. Consequently, the IFSCA on January 12, 2022, in terms of Reg.9(3) of the IIIO Regulations, 2021 read with Reg.14(2) of IRDAI (Insurance Brokers) Regulations, 2018, had directed the Noticee/ Branch office of PIBPL in GIFT IFSC, not to engage in any fresh insurance business until the renewal of CoR is granted, except for servicing the existing policyholders. The Noticee/ Branch office of PIBPL in GIFT IFSC failed to acknowledge receipt of IFSCA email dated January 12, 2022, and continued with its business operation in stark violation of the direction issued by the IFSCA. Therefore, the IFSCA on May

[41](Source: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2098153)

30, 2023 directed the Noticee/ Branch office of PIBPL in GIFT IFSC to submit certain information about their operations.

Consideration of Issues and Findings

The main issue for consideration in the instant matter is that the Noticee has not followed the directions issued by IFSCA and has acted in contravention of the regulatory requirements laid down under the IFSCA (Insurance Intermediary) Regulations, 2021.

Order

In exercise of the powers conferred under Section 12 and Section 13 of the IFSCA Act, 2019, and Regulation 30 of the IIIO Regulations, 2021 r/w Section 33(6)(b) of the Insurance Act, 1938, the validity of approval/authorization granted to PIBPL to operate "Branch office in GIFT IFSC" as IFSC Insurance Intermediary Office (IIIO) was cancelled. Irrespective of the cancellation of approval/authorization, the Noticee shall continue to be liable for anything done or omitted to be done as Insurance Intermediary and continue to be responsible for payment of outstanding fees and dues and interest, if any, due to the Authority. The Noticee shall ensure maintenance and preservation of records and other documents required to be maintained under the relevant regulations, if any.[42]

7.3 IFSCA V/S NEO Asset Management Private Limited

Facts of the Case

M/s NEO Asset Management Private Limited (IFSC Branch), (hereinafter referred to as the IFSC Branch of the Noticee) was provided registration as a Fund Management Entity, under Registered FME(Non-Retail) category, by the International Financial Services Centres Authority under IFSCA (Fund Management) Regulations, 2022 bearing registration number IFSCA/FME/II/2023-24/084 on November 22, 2023.

In the surprise visits conducted by IFSCA on July 31, 2024, and August 21, 2024, the IFSC Branch of the Noticee was found to have absence of Principal Officer and Key Management Personnel on both the occasions. The IFSC Branch of the Noticee was issued an Advisory Letter No. IFSCAIF-10RA/11/2024-Capital Markets (7), addressed to the Principal Officer, IFSC Branch, by IFSCA vide letter dated September 12, 2024, informing about the status of their office during the first two MI or surprise visits.

[42](Source: https://ifsca.gov.in/Document/Order_in_respect_of_Prowess_Insurance_Brokers_Pvt._Ltd._(PIBPL_IFSC_Branch).pdf)

In the letter, the IFSC Branch of the Noticee was advised to comply with the provisions of the Fund Management Regulations and ensure that the office premises are open with physical presence of manpower including Principal Officer and Key Managerial Personnel who are mandated to be based out of IFSC, to effectively discharge its activities, at the earliest and in any case not later than four weeks from the date of the letter i.e., September 12, 2024. Further, the IFSC Branch of the Noticee was advised to be cautious in future and ensure strict compliance with the provisions of the Fund Management Regulations, failing which same shall be subject to stringent actions under the Fund Management Regulations.

This said Advisory Letter was scanned and sent through an email dated September 12, 2024, to the Principal Officer and the Compliance Officer of IFSC Branch of the Noticee. The IFSC Branch of the Noticee was also advised to collect the physical copy of the Advisory Letter from IFSCA Head office at GIFT IFSC. The IFSC Branch of the Noticee neither collected the physical copy of abovementioned Advisory Letter from IFSCA nor acknowledged/replied to the IFSCA's email dated September 12, 2024, containing the Advisory Letter.

Post completion of the four-week period on October 12, 2024, IFSCA conducted 3rd and 4th Surprise Visits to the IFSC Branch of the Noticee on October 17, 2024, and October 24, 2024, respectively. The IFSC Branch of the Noticee was again found to be without their manpower including Principal Officer and Key Managerial Personnel on both the above-mentioned visits. 9. Based on the aforementioned facts as well as findings of the visits, the Competent Authority approved initiation of action against the Noticee for non-compliance with the IFSCA (Fund Management) Regulations, 2022.

Consideration of Issues and Findings

The main issue for consideration in the instant matter is whether the IFSC Branch of the Noticee has not followed the directions issued by IFSCA and continued to act in contravention of the regulatory requirements laid down under the IFSCA (Fund Management) Regulations, 2022.

Order

In view of the foregoing, the IFSCA, in exercise of the powers conferred in terms of Regulation 143 of the IFSCA (Fund Management) Regulations, 2022 read with Sections 12 & 13 of the IFSCA Act, 2019 r/w Section 11B of the SEBI Act, dispose of the present proceedings with a Warning to the Noticee as well as the IFSC Branch of the Noticee, to be careful in future with regard to compliances under Regulation 7(4) and Regulation 10(1) of the IFSCA (Fund Management) Regulations, 2022 or the extant Fund Management Regulations. Repetition of any of these violations shall be treated as a matter of serious concern and will result in initiation of stringent action as deemed appropriate under the provisions of IFSCA Act and applicable regulations etc.

7.4 FIU-IND V/S Way2Wealth Brokers Private Limited

Summary of Order-in-Original No. 29/DIR/FIU-IND/2022 dated 10.11.2022 in the matter of Way2Wealth Brokers Private Limited (Reporting Entity) – reg.

As part of its supervisory functions under Prevention of Money Laundering Act (PMLA), Financial Intelligence Unit-India (FIU-IND) takes up cases where apparent or potential non-compliances of relevant obligations have been observed. They are carried out with a view towards identifying weaknesses in the safeguards implemented by 'reporting entities' and for conducting enforcement activity where non-compliances are found. In relation to the securities market such actions are taken to ensure that all possible safeguards, as required by law, were effectively implemented by the reporting entities so as to ensure malicious actors do not take advantage of the capital flows therein. In this regard, FIU-IND works closely with various sectoral regulators including, the Securities and Exchange Board of India (SEBI).

Facts of the case

Based on a reference from the SEBI highlighting alleged non-compliance with PMLA guidelines by Way2Wealth Brokers Private Limited, FIU-IND had taken up the case for further analysis in order to examine whether there was any non-compliance by the reporting entity with respect to the obligations under Chapter IV of PMLA.

After examining the material on record and the submissions made, Way2Wealth Brokers Private Limited was found to have breached the relevant obligations in respect of:

- its underlying transactions in December 2021. Failure of the reporting entity to properly raise, investigate alerts, handle the alerts and to file the same as a Suspicious Transaction Report (STR) with FIU-IND;
- failure of the reporting entity to properly raise an alert and consider adverse orders of SEBI from the perspective of AML transactional monitoring and reporting obligations.

Findings of the Case & Order

- In view of the facts and due to the deficiencies observed in the mechanism implemented by the reporting entity, it was found appropriate to issue monetary penalty of Rs. 1 Lac under section 13(2)(d) to Way2Wealth Brokers Private Limited along with detailed directions to the reporting entity under section 13(2)(a) and 13(2)(b).
- Way2Wealth Brokers Private Limited was further required to return, within a period of 30 days, a certification under signature of its Designated Director and Principal Officer that the directed measures would be implemented within the periods prescribed.

7.5 FIU-IND vs Paytm Payments Bank Limited

Paytm Payments Bank Ltd. by virtue of operating as a payments bank, is a 'reporting entity' for the purposes of Section 2(l)(wa) and is registered as such with FIU-IND. A show-cause notice (SCN) numbered 9-55/2020/Compl/FIU-IND dated 14.02.2022, was issued to PayTM Payments Bank Ltd. (RE).

Issues for consideration

The inception of the current proceedings stems from the identification by law enforcement agencies of extensive illegal activity conducted by multiple businesses under the syndicate of individuals connected to a foreign state. The matter first came to light with the lodging of First Information Reports (FIRs) by the Cyber Crime Station of Hyderabad under relevant sections of the Indian Penal Code and the Telangana State Gambling Act in relation to the activities of certain business entities. The FIRs state that these entities and their network of businesses engaged in a number of illegal acts, such as organizing and assisting online gambling, and that the money obtained from these illegal operations that were proceeds of such criminal activities were routed and channeled through bank accounts maintained by the same entities with the Bank.

As part of its mandate to ensure effective implementation of Chapter IV of the PMLA, FIU- IND regularly examines the compliance levels of 'reporting entities' in the wake of any criminal conduct or fraud being reported to it or otherwise coming to light. In the course of such investigation, and as reported in the public domain, certain entities were found to have cheated lakhs of Indians through the offering of fraudulent services including prohibited gambling activities, dating services, and streaming. The proceeds of these fraudulent activities were subsequently remitted abroad. It came to light that several of the involved entities had made use of payment intermediaries to implement their fraudulent designs within the country.

Allegations and findings

The matter, and the responses of the Bank, were examined in detail by FIU-IND and it appears to be the case that the Bank has failed to discharge its obligations under Chapter IV of the PMLA. The Bank conveyed its response and after examining the material on record and the submissions made, the bank has been found to breach/violated the following relevant obligations:

Payout-related charges

a) In respect of the failure of the Bank to put in place an internal mechanism to detect and report suspicious transactions in the manner prescribed under the PMLA and PML Rules including with reference to its Payout service and accounts of the entities in question. In violation of Section 12(1) of PMLA read with Rules 3(1)(0) and 7(3).

b) In respect of the failure of the bank to exercise ongoing due diligence with respect to its Payout service and accounts of entities in question relating to the same service in violation of Section 12(1) of PMLA read with Rule 9(12);
c) In respect of failure of the Bank to satisfy the requirements with respect to reliance on third-party KYC by relying on a non-compliant/unregulated entity in violation of Section 12 of PMLA read with Rule 9(2)(c) and Rule 9(2)(f).

Beneficiary account related charges

a) In respect of failure to file suspicious transaction reports, in respect of 34 beneficiary accounts, in the manner, and within timelines, prescribed under the PMLA and PML Rules in violation of Section 12(1) of PMLA read with Rules 3(0) and Rule 8 of the PML Rules.
b) In respect of the failure of the bank to exercise ongoing due diligence with reference to the accounts of 34 beneficiaries which received proceeds from the Payout accounts of and entities in question in violation of Section 12(1) of PMLA read with Rule 9(12), PML Rules.

Order

After considering the written and oral submissions of the Bank, Director, FIU-IND, based on the material available on record, found that the charges against Paytm Payments Bank Ltd. were substantiated. Consequently, the Director FIU-IND vide order dated 15March, 2024 in exercise of his powers under Section 13 PMLA, imposed a total fine of Rs. 5,49,00,000 (Rupees Five Crore Forty-Nine Lakh Only) on the Bank with reference to the above violations committed by the Bank.

Sample Questions

1. Which of the following activities should NOT to be done by a reporting entity?
   a) Raise an alert
   b) Investigate an alert
   c) Ignore an alert
   d) File a STR

2. As per Regulatory requirement, all intermediaries should:
   a) Have an Anti Money Laundering Policy
   b) Apply customer due diligence on risk sensitive basis
   c) Appoint a Principal Officer
   d) All of the above

3. Which of the following statements about the actions of an intermediary is TRUE?
   a) Should not classify clients into High, Medium and Low risk
   b) Should close STRs without giving appropriate reasons
   c) Have a system to identify clients as a potential PEP (Politically Exposed Person)
   d) Monitor transactions without considering AML & CFT provisions.

4. Under the PMLA 2002, what is a Virtual Digital Asset Service Provider (VDA SP) classified as?
   a) Reporting Entity
   b) Regulated Entity
   c) Registered Entity
   d) Related Entity

Chapter-8 Financial Action Task Force and Its Recommendations on AML and CFT

Learning Objective- After studying this chapter, you should know about:

- Purpose of formation of FATF and initiatives taken by it to protect the global financial system from being exploited for illicit activities.
- The concept, process and preventive measures to be taken for Trade-based Money Laundering.

8.1 Introduction of FATF

The Financial Action Task Force (FATF) leads global action to tackle money laundering, terrorist and proliferation financing. The 40-member body sets international standards to ensure national authorities can effectively go after illicit funds linked to drugs trafficking, the illicit arms trade, cyber fraud and other serious crimes.

The FATF researches how money is laundered and terrorism is funded, promotes global standards to mitigate the risks, and assesses whether countries are taking effective action. In total, more than 200 countries and jurisdictions have committed to implement the FATF's Standards as part of a co-ordinated global response to preventing organised crime, corruption and terrorism. Countries and jurisdictions are assessed with the help of nine FATF Associate Member organisations and other global partners, the IMF and World Bank.

The FATF's decision-making body, the FATF Plenary, meets three times per year and holds countries to account if they do not comply with the Standards. If a country repeatedly fails to implement FATF Standards then it can be named a Jurisdiction under Increased Monitoring or a High Risk Jurisdiction. These are often externally referred to as “the grey and black lists”.

Grey List- When the FATF places a jurisdiction under increased monitoring, it means the country has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring. This list is often externally referred to as the “grey list”.

Black List- For all countries identified as high-risk by FATF, the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence, and, in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the money laundering, terrorist financing, and proliferation financing (ML/TF/PF) risks emanating from the country. This list is often externally referred to as the “black list”.

8.1.1 FATF President

The FATF President is a senior official appointed by the FATF Plenary from among its members. In April 2019, the revised Mandate extended the terms of the FATF Presidency to a two-year period.

The term of the President begins on 1 July and ends on 30 June two years after assuming office. The President convenes and chairs the meetings of the FATF Plenary and the Steering Group. The FATF Executive Secretary and FATF Secretariat staff are responsible to and act under the instructions of the President, in accordance with any directions given by the Plenary, on all issues relating to the activities and function of the FATF. The President is the principal spokesperson for the FATF and represents the FATF externally.

Elisa de Anda Madrazo of Mexico is the FATF President from 1 July 2024 to 30 June 2026. She succeeded Mr. T. Raja Kumar of Singapore.

The FATF Vice-President, is appointed by the Plenary from among its members and assists the President in carrying out his/her responsibilities. Giles Thomson of the United Kingdom assumed his role as Vice-President of the FATF on July 1, 2025.

8.1.2 Mandate of the FATF

Money laundering, terrorist financing and the financing of weapons of mass destruction are enduring concerns for the integrity of the financial system. They require a sustained political commitment to fight these threats.

This is why, in 2019, FATF Ministers gave the FATF an open-ended mandate after three decades of operation under a time-bound mandate. In 2001, the FATF expanded its mandate to also combat terrorist financing. FATF's mandate recognises the need for FATF to continue to lead decisive, co-ordinated and effective global action to counter the threats of the abuse of the financial system by criminals and terrorists, and strengthens its capacity to respond to these threats that all countries face.

8.2 FATF Recommendations

The FATF Recommendations provide a comprehensive framework of measures to help countries tackle illicit financial flows. These include a robust framework of laws, regulations and operational measures to ensure national authorities can take effective action to detect and disrupt financial flows that fuel crime and terrorism, and punish those responsible for illegal activity.

The 40 Recommendations are divided into seven distinct areas:

- AML/CFT Policies and coordination
- Money laundering and confiscation
- Terrorist financing and financing of proliferation
- Preventive measures
- Transparency and beneficial ownership of legal persons and arrangements
- Powers and responsibilities of competent authorities and other institutional measures
- International cooperation

List of these Recommendations is as follows.

Number	Old Number	
		A – AML/CFT POLICIES AND COORDINATION
1	-	Assessing risks & applying a risk-based approach *
2	R.31	National cooperation and coordination *
		B – MONEY LAUNDERING AND CONFISCATION
3	R.1 & R.2	Money laundering offence *
4	R.3	Confiscation and provisional measures *
		C – TERRORIST FINANCING AND FINANCING OF PROLIFERATION
5	SRII	Terrorist financing offence *
6	SRIII	Targeted financial sanctions related to terrorism and terrorist financing *
7		Targeted financial sanctions related to proliferation *
8	SRVIII	Non-profit organisations *
		D – PREVENTIVE MEASURES
9	R.4	Financial institution secrecy laws
		Customer due diligence and record keeping
10	R.5	Customer due diligence *
11	R.10	Record keeping
		Additional measures for specific customers and activities
12	R.6	Politically exposed persons *
13	R.7	Correspondent banking *
14	SRVI	Money or value transfer services *
15	R.8	New technologies *
16	SRVII	Payment transparency *
		Reliance, Controls and Financial Groups
17	R.9	Reliance on third parties *
18	R.15 & R.22	Internal controls and foreign branches and subsidiaries *
19	R.21	Higher-risk countries *

		Reporting of suspicious transactions
20	R.13 & SRIV	Reporting of suspicious transactions *
21	R.14	Tipping-off and confidentiality
		Designated non-financial Businesses and Professions (DNFBPs)
22	R.12	DNFBPs: Customer due diligence *
23	R.16	DNFBPs: Other measures *
24	R.33	Transparency and beneficial ownership of legal persons *
25	R.34	Transparency and beneficial ownership of legal arrangements *
		Regulation and Supervision
26	R.23	Regulation and supervision of financial institutions *
27	R.29	Powers of supervisors
28	R.24	Regulation and supervision of DNFBPs *
		Operational and Law Enforcement
29	R.26	Financial intelligence units *
30	R.27	Responsibilities of law enforcement and investigative authorities *
31	R.28	Powers of law enforcement and investigative authorities
32	SRIX	Cash couriers *
		General Requirements
33	R.32	Statistics
34	R.25	Guidance and feedback
		Sanctions
35	R.17	Sanctions
		G – INTERNATIONAL COOPERATION
36	R.35 & SRI	International instruments
37	R.36 & SRV	Mutual legal assistance
38	R.38	Mutual legal assistance: freezing and confiscation *
39	R.39	Extradition
40	R.40	Other forms of international cooperation *
	1. The 'old number' column refers to the corresponding 2003 FATF Recommendation.	
	Version as adopted on 15 February 2012.	

The FATF Recommendations are also often referred to as the FATF Standards, which comprise the Recommendations themselves and their Interpretive Notes, together with the applicable definitions in the Glossary.

As countries have diverse legal, administrative and operational frameworks and different financial systems, they should adapt the implementation of the Recommendations to their particular circumstances.

8.3 IX Special Recommendations

Recognising the vital importance of taking action to combat the financing of terrorism, the FATF has agreed these Recommendations, which, when combined with the FATF Forty Recommendations on money laundering, set out the basic framework to detect, prevent and suppress the financing of terrorism and terrorist acts.

The 40+9 Recommendations, together with their interpretative notes, provide the international standards for combating money laundering (ML) and terrorist financing (TF).

The IX Recommendations are:

I. Ratification and implementation of UN instruments

Each country should take immediate steps to ratify and to implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism.

Countries should also immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.

II. Criminalising the financing of terrorism and associated money laundering

Each country should criminalise the financing of terrorism, terrorist acts and terrorist organisations. Countries should ensure that such offences are designated as money laundering predicate offences.

III. Freezing and confiscating terrorist assets

Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organisations in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts.

Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations.

IV. Reporting suspicious transactions related to terrorism

If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organisations, they should be required to report promptly their suspicions to the competent authorities.

V. International Co-operation

Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organisations.

Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations, and should have procedures in place to extradite, where possible, such individuals.

VI. Alternative Remittance

Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions.

VII. Wire transfers

Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain.

Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number).

VIII. Non-profit organisations

Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused:

(i)	by terrorist organisations posing as legitimate entities;
(ii)	to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and
(iii)	to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

IX. Cash Couriers

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including a declaration system or other disclosure obligation.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declarations or disclosures. In cases where the currency or bearer negotiable instruments are related to terrorist financing or money laundering, countries should also adopt measures, including legislative ones consistent with Recommendation 3 and Special Recommendation III, which would enable the confiscation of such currency or instruments.

The cornerstone of the FATF 40+9 Recommendations is the risk-based approach which emphasizes the need for countries to identify and understand the money laundering and terrorist financing risks they are exposed to. This ensures they can prioritise their resources to mitigate risks in the highest risk areas. The FATF continuously monitors new and evolving threats to the financial system and regularly updates and refines its Recommendations so that countries have up-to-date tools to go after criminals.

To help countries implement its Standards, the FATF also creates guidance and best practice papers on range of issues. The FATF regularly revises them to reflect the experience gained by public authorities and private sector over the years so that countries can benefit from this experience and effectively implement the FATF Recommendations in their own national context. This process can involve outreach to stakeholders or public consultations to ensure the usefulness of the final report.

8.4 FATF-Style Regional Bodies (FSRBs)

Nine FATF-Style Regional Bodies have been established. The FATF-style regional bodies are:

i. Asia/Pacific Group on Money Laundering (APG) based in Sydney, Australia;
ii. Caribbean Financial Action Task Force (CFATF) based in Port of Spain, Trinidad and Tobago;
iii. Eurasian Group (EAG) based in Moscow, Russia;
iv. Eastern & Southern Africa Anti-Money Laundering Group (ESAAMLG) based in Dar es Salaam, Tanzania;
v. Central Africa Anti-Money Laundering Group (GABAC) based in Libreville, Gabon;
vi. Latin America Anti-Money Laundering Group (GAFILAT) based in Buenos Aires, Argentina;
vii. West Africa Money Laundering Group (GIABA) based in Dakar, Senegal;
viii. Middle East and North Africa Financial Action Task Force (MENAFATF) based in Manama, Bahrain;
ix. Council of Europe Anti-Money Laundering Group (MONEYVAL) based in Strasbourg, France (Council of Europe).

The APG, in conjunction with the FATF and the other eight regional bodies, constitute a global network to combat money laundering, the financing of terrorism and the financing of proliferation of weapons of mass destruction. The FATF's 40 recommendations are the principal standards to combat these crimes.

With the above discussion it is understandable that FATF promotes sharing of best practices, guides reforms in member and non-member states, and updates standards to address risks from emerging threats such as cryptocurrencies and proliferation financing. FATF's framework is widely adopted, boosting the transparency of financial systems, making it harder for criminals and terrorists to move, hide, or use funds undetected.

8.5 What is Trade-based Money Laundering?

Trade-based money laundering is defined as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins.

There are three main methods by which criminal organisations and terrorist financiers move money for the purpose of disguising its origins and integrating it into the formal economy.

i. The first involves the movement of value through the financial system using methods such as cheques and wire transfers;
ii. The second involves the physical movement of banknotes using methods such as cash couriers and bulk cash smuggling; and
iii. The third involves the movement of value using methods such as the false documentation and declaration of traded goods and services.

Each of these methods involves the movement of enormous volumes of funds and can operate at a domestic or international level. In recent years, the Financial Action Task Force has focused considerable attention on the first two of these methods. By comparison, the scope for abuse of the international trade system has received relatively little attention.

Over the past few years, the Financial Action Task Force (FATF) has focused considerable attention on the first two of these methods. In 2003, the FATF significantly toughened the standards that apply to the financial system and various non-financial intermediaries. Two years later, it extended these standards to cover the activities of cash couriers. To date, however, limited attention has been focused on trade-related activities. Not surprisingly, research has shown that when governments take action against certain methods of money laundering or terrorist financing, criminal activities tend to migrate to other methods. In part, this reflects the fact that more aggressive policy actions and enforcement measures increase the risk of detection and therefore raise the economic cost of using these methods.

This suggests that the FATF's recent actions to revise the 40 Recommendations on money laundering and extend the 8 Special Recommendations on terrorist financing to cover cash couriers, as well as the ongoing efforts of countries to implement these stricter standards, may have the unintended effect of increasing the attractiveness of the international trade system for money laundering and terrorist financing activities.

8.6 The International Trade System

The international trade system is subject to a wide range of risks and vulnerabilities, which provide criminal organisations with the opportunity to launder the proceeds of crime and provide funding to terrorist organisations, with a relatively low risk of detection. The relative attractiveness of the international trade system is associated with:

- The enormous volume of trade flows, which obscures individual transactions and provides abundant opportunity for criminal organisations to transfer value across borders;
- The complexity associated with (often multiple) foreign exchange transactions and recourse to diverse financing arrangements;

- The additional complexity that can arise from the practice of commingling illicit funds with the cash flows of legitimate businesses;
- The limited recourse to verification procedures or programs to exchange customs data between countries; and
- The limited resources that most customs agencies have available to detect illegal trade transactions.

On this last point, research suggests that most customs agencies inspect less than 5 percent of all cargo shipments entering or leaving their jurisdictions. In addition, most custom agencies are able to direct relatively limited analytical resources to improved targeting and identification of suspicious trade transactions.

In recent decades, international trade has grown significantly: global merchandise trade now exceeds US$9 trillion a year and global trade in services accounts for a further US$2 trillion3. Much of this trade is associated with the financial system, as a significant amount of goods and services are financed by banks and other financial institutions. In industrial countries the growth of trade has significantly exceeded the growth of gross domestic product, while in developing countries it has increased even faster. In addition, virtually all economies have become more open to trade. This has placed increasing pressure on the limited resources that most countries, especially developing countries, have available to scrutinise these activities.

8.6.1 Abuse of the International Trade System

Researchers have documented how the international trade system can be used to move money and goods with limited scrutiny by government authorities. In addition to money laundering, a considerable amount of academic attention has focused on the related activities of tax avoidance and evasion, and capital flight. A brief review of the recent literature in these areas is provided below.

a) Tax Avoidance and Evasion

The differing tax rates have an impact on the incentives of corporations to shift taxable income from jurisdictions with relatively high tax rates to jurisdictions with relatively low tax rates in order to minimise income tax payments.

b) Capital Flight

Companies and individuals also shift money from one country to another to diversify risk and protect their wealth against the impact of financial or political crises. Several of these studies also show that a common technique used to circumvent currency restrictions is to over-invoice imports or under invoice exports.

c) Trade-Based Money Laundering

Unlike tax avoidance and capital flight, which usually involve the transfer of legitimately earned funds across borders, capital movements relating to money laundering – or trade-based money laundering – involve the proceeds of crime, which are more difficult to track. A number of studies have analyzed techniques to establish whether reported import and export prices reflect fair market values. One of the methods currently being explored involves the use of statistical techniques to detect discrepancies in the information provided on shipping documents to better identify suspicious trading activity.

8.6.2 Basic Trade-Based Money Laundering Techniques

The basic techniques of trade-based money laundering include:

- over- and under-invoicing of goods and services;
- multiple invoicing of goods and services;
- over- and under-shipments of goods and services; and
- falsely described goods and services.

However, it may be noted that all of these techniques are not necessarily in use in every country.

a) Over- and Under-Invoicing of Goods and Services

Money laundering through the over- and under-invoicing of goods and services, which is one of the oldest methods of fraudulently transferring value across borders, remains a common practice today. The key element of this technique is the misrepresentation of the price of the good or service in order to transfer additional value between the importer and exporter.

By invoicing the good or service at a price below the “fair market” price, the exporter is able to transfer value to the importer, as the payment for the good or service will be lower than the value that the importer receives when it is sold on the open market. Alternatively, by invoicing the good or service at a price above the fair market price, the exporter is able to receive value from the importer, as the payment for the good or service is higher than the value that the importer will receive when it is sold on the open market.

b) Multiple Invoicing of Goods and Services

Another technique used to launder funds involves issuing more than one invoice for the same international trade transaction. By invoicing the same good or service more than once, a money launderer or terrorist financier is able to justify multiple payments for the same shipment of goods or delivery of services. Employing a number of different financial institutions to make these additional payments can further increase the level of complexity surrounding such transactions.

c) Over- and Under-Shipments of Goods and Services

In addition to manipulating export and import prices, a money launderer can overstate or understate the quantity of goods being shipped or services being provided. In the extreme, an exporter may not ship any goods at all, but simply collude with an importer to ensure that all shipping and customs documents associated with this so called "phantom shipment" are routinely processed. Banks and other financial institutions may unknowingly be involved in the provision of trade financing for these phantom shipments.

d) Falsely Described Goods and Services

In addition to manipulating export and import prices, a money launderer can misrepresent the quality or type of a good or service. For example, an exporter may ship a relatively inexpensive good and falsely invoice it as a more expensive item or an entirely different item. This creates a discrepancy between what appears on the shipping and customs documents and what is actually shipped. The use of false descriptions can also be used in the trade in services, such as financial advice, consulting services and market research. In practice, the fair market value of these services can present additional valuation difficulties.

8.6.3 Complex Trade-Based Money Laundering Techniques

In practice, strategies to launder money usually combine several different techniques. Often these involve abuse of both the financial and international trade systems. Black market peso exchange arrangements is one such Complex Trade-based Money Laundering technique that provides a useful illustration of how a number of different money laundering techniques can be combined into a single criminal operation. These transactions combine a number of different illegal activities, such as drug smuggling, money laundering through the financial system and trade-based money laundering.

Unlike the basic trade-based money laundering techniques discussed above, there is also no need for the importer and exporter to collude in a fraudulent transaction for the black market peso exchange arrangement to work. Instead, the prices and quantities of the goods can be correctly reported to customs agencies and value can still be transferred across borders. Although the term "black market peso exchange" refers to a money laundering technique that was originally associated with Colombian narcotics trafficking, these arrangements are widely used in many countries to repatriate the proceeds of various types of crimes.

8.6.4 Current Practices

The international trade system is subject to a wide range of vulnerabilities that can be exploited by criminal organisations and terrorist financiers. To examine the capacity of national authorities to combat trade-based money laundering, the FATF project team has made use of a detailed questionnaire to survey current practices in a range of countries. This questionnaire focuses on the ability of various government agencies to identify suspicious activities related to trade transactions, to share this information with domestic and foreign partner agencies, and to act on this information. In carrying out this work, particular attention has been focused on the practices of customs agencies, law enforcement agencies, financial intelligence units, tax authorities and banking supervisors.

Looking ahead, there appears to be a number of practical steps that could initially be taken to improve the capacity of national authorities to cope with trade-based money laundering. These can be summarised as follows:

a) **Building Better Awareness**: The review of current practices of those countries responding to the FATF questionnaire showed that there was almost unanimous agreement on the need for a stronger focus on training programs for competent authorities (e.g., customs agencies, law enforcement agencies, financial intelligence units, tax authorities and banking supervisors) to better identify trade-based money laundering techniques. In turn, improved training could result in substantial increases in the number of suspicious transaction reports filed with financial intelligence units. In addition, such training programs could be usefully supplemented by outreach sessions to the private sector.

b) **Strengthening Current Measures**: There are a number of actions that countries could take to better identify trade-based illicit activity. The simplest is to ensure that competent authorities and financial institutions have access to the case studies and red flag indicators in this study. In addition, most countries would benefit from more effective information sharing among competent authorities at the domestic level. For example, it would be useful if law enforcement agencies could seek information from customs agencies on specific trade transactions in advance of a full-fledged criminal investigation.

c) **Improving International Co-operation**: Countries need to work cooperatively to identify and combat trade-based money laundering. Consistent with FATF standards, countries could put clear and effective gateways in place to facilitate the prompt and constructive exchange of information. In practice, this may require broader use of memoranda of understanding and mutual legal assistance treaties between countries to facilitate the sharing of information related to specific transactions. It also means greater recourse to mutual assistance agreements between customs agencies to facilitate the exchange of export and import data in order to identify trade anomalies that may indicate potential trade-based money laundering abuses.

Sample Questions

1. The process of disguising the proceeds of crime and moving value through the use of trade transactions is better known as?
   a) Bulk cash smuggling
   b) Cheques and wire transfers
   c) Trade-based Money Laundering
   d) All of the above

2. The criminal organizations are more prone to misuse the international trade system due to which of the following reasons?
   a) Minimum volumes of trade flows
   b) The limited resources available for detection of illegal trades
   c) Least complexity of foreign exchange transactions.
   d) Easy exchange of customs data between the countries.

3. When Companies shift money from one country to another to diversify risk and protect their wealth against the impact of financial or political crises, what is the process better known as?
   a) Capital Flight
   b) Tax Avoidance and Evasion
   c) Trade-based Money Laundering
   d) Anti Money Laundering.

4. Which of the following measures would most effectively strengthen international cooperation to combat trade-based money laundering (TBML) in line with FATF standards?
   a) Restricting cross-border trade transactions through higher customs duties
   b) Establishing clear information-sharing gateways through MOUs, Mutual Legal Assistance Treaties, and customs-to-customs cooperation for exchange of trade data
   c) Conducting unilateral investigations without involving foreign jurisdictions
   d) Limiting reporting obligations only to domestic financial institutions

Additional Reads

1) Frequently Asked Questions (FAQs) on International Financial Services Centres Authority (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022.

2) UAPA Order - Gazette Notification 4391(E) dated October.10.2024

3) UBO Identification dated September 08, 2023.

******

NATIONAL INSTITUTE OF SECURITIES MARKETS

NISM Registered Office
5th floor, NCL Cooperative Society,
Plot No. C-6, E-Block, Bandra Kurla Complex,
Bandra East, Mumbai, 400051
Tel: +91-22-41738811

NISM Campus
Plot No. IS 1 & 2, Patalganga Industrial Area,
Mohopada, District Raigad,
Maharashtra–410222
Tel: +91-2192-668300

NISM Bhavan
Plot No. 82, Sector–17,
Vashi, Navi Mumbai, Maharashtra–400703
Tel: +91-22-66735100/5101
Fax: 022-66735110

www.nism.ac.in