

Financial Crime and Compliance (FCC)

For AIBB

First Edition: September 2023

Second Edition: March 2024

Third Edition: June 2024

Fourth Edition: January 2025

Fifth Edition: June 2025

Do not copy or share this material; the author worked hard on it and holds the copyright.

Edited By:

Mohammad Samir Uddin, CFA

Chief Executive Officer

MBL Asset Management Limited

Former Principal Officer of EXIM Bank Limited

CFA Chartered from CFA Institute, U.S.A.

BBA, MBA (Major in finance) From Dhaka University

Qualified in Banking Diploma and Islami Banking Diploma

Course instructor: 10 Minute School of 96th BPE

Founder: MetaMentor Center, Unlock Your Potential Here.

Price: 350Tk.

For Order:

www.metamentorcenter.com

WhatsApp: 01310-474402



**Metamentor Center
Unlock Your Potential Here.**

Table of Content

SL	Details	Page No.
1	Module-A: Conceptual Issues and Terminology	4-21
2	Module-B: Financial Crime in the Key Functional Areas of Banking	22-30
3	Module-C: Financial Crime Risk Assessment	31-45
4	Module-D: Prevention, Detection and Reporting	46-66
5	Module-E: Sanctions, Anti-Bribery and Corruption	67-78
6	Module-F: Financial Crime Control (FCC) for New Economy	79-82
7	Module-G: Compliance	83-91
	Short Note	91-106
9	<i>Previous year Question</i>	106-112

Suggestion:

- *Read 4 star and 5 star marked chapter if you have time shortage to read all chapter.*
 - *Must read short notes from all chapter.*
- *MetaMentor Center suggest to read whole note to find 100% common in exam. We cover everything in our note.*

Important	Details	Number of Question common in previous years
*****	Module-A: Conceptual Issues and Terminology	32
**	Module-B: Financial Crime in the Key Functional Areas of Banking	11
****	Module-C: Financial Crime Risk Assessment	12
*****	Module-D: Prevention, Detection and Reporting	32
*****	Module-E: Sanctions, Anti-Bribery and Corruption	16
*	Module-F: Financial Crime Control (FCC) for New Economy	1
**	Module-G: Compliance	11

Syllabus-2025

Module-A: Conceptual Issues and Terminology

Financial Crime, Nature of Financial Crime, Key stakeholders of Financial Crime, Money Laundering, Terrorist Financing, Sanctions, Bribery and Corruption. Predicate Offence, Reporting Organizations, Investigative Agencies, Stages of ML, Bangladesh Financial Intelligence Unit (BFIU), FATF, APG, Egmont Group, National Coordination Committee and National Taskforce on AML- CFT, Penalties.

Module-B: Financial Crime in the Key Functional Areas of Banking

Nature of crimes in General Banking, Fraud and forgeries in Credit Operations, Malpractices and crime in Trade Services and Foreign Exchange, Internal Control and Compliance (ICC) functions of banks and Financial Crime.

Module-C: Financial Crime Risk Assessment

ML/TF Risk Assessment Guidelines for Banking Sector; Identifying and Assessing Trade Based Money Laundering (TBML), Guidelines for Trade Based Money Laundering in Bangladesh; Enterprise-wide, Business, Sector and Product level FC Risk; Geographic Risk, FATF Blacklists and Gray-lists.

Module-D: Prevention, Detection and Reporting

Customer, Beneficial Owner, Customer Acceptance Policy, KYC, Customer Risk Assessment/Rating, Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), Periodic and Adhoc CDD/EDD review, Name Screening; Transaction Profile (TP), Transaction Monitoring, TP Based Transaction Monitoring, Automated Transaction Monitoring, Manual Transaction Monitoring, Transaction Screening, Ongoing Name Screening, Media Monitoring. Self-Assessment, Cash Transaction Reporting (CTR), Suspicious Transaction Reporting (STR), Suspicious Activity Reporting (STR), Protection for good faith reporting, Reporting for Internal Governance, Negative Lists

Module-E: Sanctions, Anti-Bribery and Corruption

Economic Sanctions, Various Types of Sanctions, US Sanctions, UN Sanctions, Bangladesh list, Bribery, Corruption, Important definitions and provisions of Anti-Corruption Commission Act, 2004, Penal Code provisions on Bribery, expatriation of corruption proceeds, Bribery & Corruption through employment, internship, gifts, procurement, sponsorship and donations.

Module-F: Financial Crime Control (FCC) for New Economy

FCC Risk Associated with new services and Technology, Fintech products, MFS, e-wallet, transactional platforms, e-commerce sites, marketplace; Money Laundering in the New Payment System.

Module-G: Compliance

Concepts of Compliance and Compliance Risk, Identifying and Managing Compliance Risk, Various Sub-Risks, Assessing Inherent and Residual Compliance Risk, Compliance Policies and Governance, Regulatory Compliance, Independence of Compliance Function and role of all employees and senior management for compliance.

Module A:

Conceptual Issues and Terminology

Q-01. What is financial crime? What type of financial crimes/ common forms of financial 5 crime are observed in Bangladesh financial sector? BPE-96th. BPE-98th. BPE-99th.

Financial crime involves illegal activities to gain economic benefits through dishonest means, often using financial systems. Key types of financial crimes include fraud, corruption, tax evasion, insider trading, loan scams, and money laundering. In Bangladesh's financial sector, notable financial crimes include:

- 1. Fraud and Forgery:** Deceiving others for financial gain.
- 2. Corruption and Bribery:** Illegal benefits in exchange for influence or action in business or government.
- 3. Tax Evasion:** Illegally avoiding paying taxes.
- 4. Insider Trading and Market Manipulation:** Using confidential information for trading or manipulating market prices.
- 5. Loan Scam:** Obtaining loans through false pretenses.
- 6. Money Laundering:** Hiding the origins of illegally obtained money.
- 7. Terrorist Financing:** Funding terrorist activities.
- 8. Proliferation Financing of Weapons of Mass Destruction (WMD):** Financial support for developing WMDs.
- 9. Online Gaming and Betting:** Illegal or unregulated online gambling.
- 10. Hundi/Hawala:** Informal methods of transferring money, often bypassing legal channels.

These crimes impact the financial stability and trust in institutions, contributing to broader social and economic issues.

Q-02. Which are the main stakeholders of countering financial crimes in Bangladesh?

In Bangladesh, the main stakeholders involved in countering financial crimes include:

- 1. Reporting Organizations (ROs):** Entities required to report suspicious financial activities.
- 2. Bangladesh Financial Intelligence Unit (BFIU):** Central agency for analyzing financial transactions related to illegal activities.
- 3. Investigating Agencies:** Such as the Anti-Corruption Commission (ACC), Criminal Investigation Department (CID) of Bangladesh Police, Bangladesh Securities and Exchange Commission (BSEC), Customs Intelligence and Investigation Directorate (CIID), Central Intelligence Cell (CIC) of National Board of Revenue, Department of Narcotics Control (DNC), and Directorate of Environment.
- 4. Intelligence Agencies:** Engaged in gathering information related to financial crimes.
- 5. Regulatory Authorities:** Including Bangladesh Bank, BSEC, Insurance Development and Regulatory Authority (IDRA), NGO Affairs Bureau, Microcredit Regulatory Authority (MRA), Department of Social Services, and Self-Regulatory Bodies.
- 6. Different Ministries:** Like the Ministry of Commerce, Ministry of Finance, Ministry of Information Technology and Communication, and Ministry of Telecommunication.

These stakeholders play crucial roles in identifying, reporting, investigating, and regulating activities to combat financial crimes effectively.

Q-03. "All money laundering cases are financial crime but all financial crime are not money laundering" please discuss with some examples. BPE-96th. BPE-99th.

"Money laundering is a specific type of financial crime, but not all financial crimes are money laundering." This means while every act of money laundering is a financial crime, there are many financial crimes that are not related to money laundering.

Example of Money Laundering (Financial Crime): Suppose someone earns money illegally, maybe by selling drugs. They then try to hide this money's illegal source by passing it through various bank accounts or businesses, making it look like it came from a legal source. This process is money laundering.

Example of Non-Money Laundering Financial Crime: A person committing tax evasion by not reporting their full income to avoid paying the correct amount of tax is committing a financial crime. However, this is not money laundering, as they are not trying to disguise the source of their money.

So, while money laundering always counts as a financial crime, there are many other types of financial crimes like tax evasion, fraud, and insider trading that don't involve laundering money.

Q-04. How a bank can be involved in a money laundering case of its customer? Describe with example. BPE-97th.

A bank can become involved in a customer's money laundering case by acting as an instrumentality, either knowingly or unknowingly, in the process of handling funds that are the proceeds of a crime. This involvement can happen when the bank is used to deposit, transfer, or withdraw money that has been obtained through illegal activities, with the intention of making these funds appear legitimate.

Example: A customer who has earned money through illegal means, such as drug trafficking, might deposit this money into a bank account. They might then perform a series of complex transactions, such as transferring the money between different accounts, possibly in various countries, or investing it in legitimate businesses. If the bank does not perform adequate checks to identify the suspicious nature of these transactions, it can become an unwitting participant in the money laundering process. The bank's systems and services are thus used to give the illegal funds an appearance of legitimacy, making it difficult for authorities to trace the original source of the money.

Q-05. How many ways financial institutions can be involved in financial crime?

Financial institutions can be involved in financial crime in three main ways:

- 1. As a Victim:** Here, the institution itself is targeted by criminals. Examples include frauds like misrepresentation of financial information, embezzlement, and various types of scams like check fraud, credit card fraud, securities fraud, and pension fraud. The institution suffers losses due to these deceptive practices.
- 2. As a Perpetrator:** In this less common scenario, the financial institution itself commits the crime. This could involve activities like selling fraudulent financial products, self-dealing, or misappropriating client funds.
- 3. As an Instrumentality:** This is when financial institutions, either knowingly or unknowingly, are used as tools or channels for criminal activities. A prime example is

money laundering, where illegal funds are processed through the institution to make them appear legitimate.

In each of these roles, the involvement of financial institutions can vary in intent and awareness, from being directly targeted to unknowingly facilitating criminal activities.

Q-06. Is there any difference between money laundering and financial crime? What are those? BPE-97th.

Aspect	Money Laundering	Financial Crime
1.Definition	A process where illegal funds are made to appear legitimate.	Broad category of crimes involving illegal gain or loss of money.
2.Purpose	To conceal the origins of illegally obtained money.	To obtain money, assets, or other property illegally.
3.Methods	Involves three stages: placement, layering, and integration.	Includes fraud, embezzlement, tax evasion, and more.
4.Legal Framework	Governed by specific anti-money laundering laws and regulations.	Covered by a wider array of laws related to financial misconduct.
5.Impact	Primarily affects the financial system and economy's integrity.	Has a broader impact, affecting individuals, businesses, and national economies.
6.Example	Laundering drug trafficking proceeds through a legitimate business.	Insider trading based on non-public information for personal gain.

Q-07. What is money laundering? Define money laundering as per MLPA, 2012. BPE-97th.

Money laundering is the process of making illegally obtained money (like from drug trafficking or corruption) appear legal. According to the Money Laundering Prevention Act (MLPA), 2012 of Bangladesh, money laundering includes several key activities:

- 1. Movement, Conversion, or Transfer of Illegal Proceeds:** This involves taking money gained from crimes and moving, converting, or transferring it to hide its illegal origin.
- 2. Concealing Illicit Nature, Source, or Ownership:** This is about hiding the true identity, source, or ownership of criminal proceeds.
- 3. Assistance in Evading Legal Consequences:** Helping someone involved in a crime to escape legal responsibility.
- 4. Smuggling Money:** Transferring or bringing money into or out of the country illegally.
- 5. Avoiding Reporting Requirements:** Conducting financial transactions in a way to dodge the legal obligation to report them.

The MLPA, 2012 essentially defines money laundering as activities that hide the illegal source of money or help criminals avoid getting caught.

Q-08. Describe the money laundering process. BPE-97th.

Or, Discuss the stages of money laundering. BPE-96th. BPE-5th.

The money laundering process involves three key stages:

- 1. Placement Stage:** This is where proceeds of crime are first introduced into the financial system, through methods like cash deposits in banks, small or structured deposits to avoid

detection, buying foreign currency, or mixing illegal funds with legitimate business revenues.

2. **Layering Stage:** The aim here is to obscure the origin of the money through complex transactions. This may include transferring funds between accounts or countries, investing in businesses, or making various financial investments that disguise the money's source.
3. **Integration Stage:** The final step reintegrates the laundered money into the economy in a manner appearing legitimate. This could be through loans, investments in real estate or luxury goods, or using it as collateral, effectively hiding the money's criminal origins and allowing it to be used without suspicion.

Q-09. A government employee named Mr. X took 50 lac BDT as bribe from a person in exchange of providing service. Then he kept 25 lac BDT in a safe place of his house and gave the rest to his brother-in-law, Mr. Y deposited the money in his own bank account in the bank HP Bank Ltd. a. Is it falls under money laundering? Give reason for your answer. b. In the above scenario, who will be charged for money laundering and why? c. What due diligence measures should be taken by the bank HP Bank Ltd?

a. Yes, this falls under money laundering. Money laundering involves disguising money obtained from illegal activities as legitimate. Mr. X acquiring money through bribery (an illegal activity) and attempting to legitimize it by depositing part of it into a bank account through Mr. Y constitutes money laundering.

b. Both Mr. X and Mr. Y could be charged for money laundering. Mr. X for initiating the process by obtaining illegal funds and attempting to disguise its origin, and Mr. Y for aiding in this process by depositing the money into his bank account, acting as a layer to separate the funds from their illegal source.

c. HP Bank Ltd. should implement strict due diligence measures including:

- Identifying and verifying the source of large deposits.
- Monitoring transactions for unusual or suspicious activity.
- Reporting suspicious activities to relevant authorities.
- Training staff to recognize signs of money laundering.

These measures help in detecting and preventing money laundering activities.

Q-10. Is it essential to follow all stages to complete money laundering offences? If not please describe with example. BPE-96th.

No, it's not essential to follow all stages to complete a money laundering offense. Money laundering typically involves three stages: placement, layering, and integration. However, a money laundering offense can occur even if not all stages are completed.

For example, if an individual gains money illegally and just deposits it into a bank account (placement), it's already considered money laundering, even if they don't proceed to disguise the origins of the money (layering) or integrate it into the economy as legitimate (integration). The mere act of introducing illicit funds into the financial system can constitute a money laundering offense, demonstrating that completion of all stages is not a prerequisite for the offense to occur.

Q-11. What is smuggling of money or asset? Elaborate your answer in line with MLPA, 2012. What is the difference between smuggling of money or asset with money laundering?

Smuggling of money or assets refers to the illegal movement of goods, currency, or other assets across borders to avoid taxes or for other criminal purposes. Under the Money Laundering Prevention Act (MLPA), 2012, this activity is closely associated with money laundering as it often involves the concealment or transfer of illicit funds.

The MLPA, 2012 defines money laundering as any process that disguises illegal gains as legitimate. Smuggling money or assets typically serves this purpose by moving illicit funds out of the country or bringing in assets that are not declared to customs, thereby evading taxes or scrutiny. This act not only violates customs and tax laws but also contributes to the laundering of money, as it obscures the illegal origin of these funds or assets, integrating them into the legal economy.

Aspect	Smuggling of Money or Assets	Money Laundering
1.Definition	The illegal movement of goods, currency, or assets across borders to avoid taxes or for other criminal purposes.	The process of making large amounts of money generated by a criminal activity, such as drug trafficking or terrorist funding, appear to be legal.
2.Primary Objective	To evade taxes or move illegal goods/cash across borders.	To disguise the origins of criminally derived funds.
3.Legal Violation	Customs and border control laws.	Laws against financial crimes, specifically those designed to conceal illicit funds' origins.
4.Detection Point	At borders or points of entry/exit.	Within the financial system, during transactions or account activities.
5.Example	Smuggling \$1 million in cash across a border to evade taxes.	Laundering \$1 million from drug sales through a legitimate business to integrate it as clean money.

Q-12. What are the responsibilities of ROS mentioned in section 25 of Money Laundering Prevention Act (MLPA), 2012? BPE-96th. BPE-98th. BPE-5th.

Under Section 25 of the Money Laundering Prevention Act (MLPA), 2012, in Bangladesh, the responsibilities of Reporting Organizations (ROs) include:

- 1. Diligent Reporting:** ROs must report any transaction suspected of being related to money laundering or terrorist financing to the Bangladesh Financial Intelligence Unit (BFIU) promptly.
- 2. Record Keeping:** They are required to keep all identification records and transaction data for a period specified by the act, typically five years, to assist in any investigation or analysis related to money laundering or terrorist financing.
- 3. Compliance Program Implementation:** ROs need to implement effective programs to combat money laundering and terrorist financing, including internal policies, procedures, and controls.
- 4. Employee Training:** Ensuring that their employees are trained to recognize and handle transactions that may involve money laundering or terrorist financing risks appropriately.

These responsibilities aim to strengthen the fight against money laundering and terrorist financing by promoting vigilance and cooperation among financial and non-financial institutions.

Q-13. Which non-compliant issues of ROS are punishable under MLPA, 2012? BPE-96th.

Under the Money Laundering Prevention Act (MLPA), 2012, in Bangladesh, non-compliant issues of Reporting Organizations (ROs) that are punishable include:

1. **Failure to Report:** Not reporting transactions suspected of money laundering or terrorist financing to the Bangladesh Financial Intelligence Unit (BFIU).
2. **Inadequate Record-Keeping:** Failing to maintain proper records of identification and transaction data for the required period.
3. **Non-Compliance with Due Diligence:** Not conducting due diligence on customers or failing to verify their identity appropriately.
4. **Lack of Compliance Program:** Not implementing a comprehensive program to prevent money laundering and terrorist financing, including policies, controls, and procedures.
5. **Negligence in Training:** Failing to train employees on recognizing and dealing with transactions related to money laundering and terrorist financing.

Violations of these responsibilities can lead to penalties, including fines and imprisonment, as outlined in the MLPA, 2012.

Q-14. What is the punishment for money laundering offence conducted by a person? BPE-97th.

Or, Mention the penal provisions in case of failure to perform those responsibilities BPE-98th.

Under the Money Laundering Prevention Act, 2012, in Bangladesh, the punishment for an individual involved in money laundering offences includes:

- **Imprisonment:** A minimum of 4 years and up to 12 years.
- **Fine:** A fine equivalent to twice the value of the property involved in the offence or 10 lakh Bangladeshi Taka (whichever is greater). If the fine is not paid, additional imprisonment equivalent to the fine may be imposed.
- **Property Forfeiture:** The court may also order the forfeiture of the convicted person's property in favor of the State if it is directly or indirectly involved in or related to money laundering or any predicate offence.

This framework emphasizes the severity with which the Bangladesh legal system treats money laundering, aiming to deter individuals and entities from engaging in such illicit activities.

Q-15. What is predicate offence? Mention 10 (ten) predicate offence. Which agencies are empowered to investigate money laundering cases? BPE-98th . BPE-5th.

A predicate offence refers to a crime that generates proceeds that can be laundered or used to finance other illegal activities. According to the Money Laundering Prevention Act (MLPA), 2012 of Bangladesh, predicate offences include a variety of criminal acts such as corruption, bribery, fraud, forgery, illegal trade of firearms, narcotics trafficking, kidnapping, murder, human trafficking, and more. These offences are recognized as the underlying crimes whose proceeds are subsequently laundered, forming the basis for money laundering investigations and prosecutions.

Here are ten examples:

1. **Fraud** – Deceptive practices for financial gain.
2. **Drug Trafficking** – Illegal distribution of controlled substances.
3. **Human Trafficking** – Exploiting people for labor or sex.
4. **Terrorism** – Violent acts to instill fear for political purposes.
5. **Corruption** – Abuse of power for personal gain.
6. **Tax Evasion** – Illegally avoiding paying taxes.
7. **Embezzlement** – Misappropriation of funds.
8. **Bribery** – Offering or receiving undue rewards.

9. Extortion – Obtaining something through force or threats.

10. Counterfeiting – Producing fake goods or currency.

These offenses often underpin more complex criminal enterprises.

Under the Money Laundering Prevention Act 2012 and related rules, several agencies are empowered to investigate money laundering cases in Bangladesh. These include:

In Bangladesh, under the Money Laundering Prevention Act 2012 and related rules, several agencies are empowered to investigate money laundering cases. These include:

1. Bangladesh Bank, particularly through its Bangladesh Financial Intelligence Unit (BFIU).
2. The Anti-Corruption Commission (ACC).
3. Law enforcement agencies like the Police, Rapid Action Battalion (RAB), and Border Guard Bangladesh (BGB).

These agencies work together to detect, investigate, and prevent money laundering, ensuring that individuals or entities cannot illegally disguise the origins of criminally obtained money.

Q-16. What is BFIU? What are the main functions and responsibilities of BFIU? BPE-97th. Or, What are the roles of Bangladesh Financial Intelligence Unit (BFIU) to prevent money laundering? BPE-98th. BPE-99th. BPE-5th.

The Bangladesh Financial Intelligence Unit (BFIU) is a central agency established under the Money Laundering Prevention Act (MLPA) 2002, renamed in 2012, focusing on combating money laundering (ML), terrorist financing (TF), and proliferation financing (PF) of weapons of mass destruction (WMD).

1. **Analysis & Reporting:** Receives, analyzes, and produces financial intelligence from STRs/SARs, CTRs, and complaints for investigative agencies.
2. **Database Management:** Maintains comprehensive databases of STRs/SARs and CTRs.
3. **Guidance & Supervision:** Issues guidelines to prevent ML, TF, and PF; supervises reporting organizations for compliance.
4. **International Compliance:** Monitors implementation of UN Security Council Resolutions on PF and cooperates with global organizations like FATF and EGMONT Group.
5. **Training & Cooperation:** Provides training and works with various stakeholders including regulators, law enforcement, and international FIUs.
6. **Policy Implementation:** Acts as secretariat for national committees on AML & CFT and monitors policy implementation.
7. **Public Awareness:** Creates awareness against ML, TF, and PF activities.

These points encapsulate the broad and critical role of the BFIU in preventing financial crimes and enhancing national and international security efforts.

Q-17. What are the powers and responsibilities of Bangladesh Bank under sections 15 and 20A of the Anti-Terrorism Act (ATA), 2009 regarding suspicious transactions?

1. **Report Analysis:** Request and analyze suspicious transaction reports.
2. **Account Freeze:** Freeze accounts for 30 days, extendable up to 6 months for terrorism-linked suspicions.
3. **Agency Supervision:** Supervise reporting agencies' activities.
4. **Preventive Directions:** Instruct on preventing terrorism financing and WMD proliferation.
5. **Compliance Monitoring:** Conduct compliance checks and on-site inspections.

6. **Training Provision:** Train in identifying suspicious transactions and preventing terrorism financing.
7. **Law Enforcement Cooperation:** Inform and collaborate with law enforcement on investigations.
8. **International Cooperation:** Seize accounts for foreign offenses or under international agreements, with fund disposal according to court or international directives.

Q-18. What kind of report bank has to report to BFIU? For how many days an account can be frozen by BFIU? BPE-97th. BPE-99th.

Based on the provided information from the authorities and responsibilities of the Bangladesh Financial Intelligence Unit (BFIU) as mentioned in the MLPA, 2012, and ATA, 2009, here are the key points regarding your questions:

1. **Type of Reports Banks Must Submit to BFIU:** Banks, as reporting organizations, are required to submit two primary types of reports to the BFIU:
 - **i. Cash Transaction Reports:** These are reports of significant cash transactions that occur within the bank.
 - **ii. Suspicious Transaction Reports:** These reports are filed when a bank identifies a transaction that appears unusual or suspicious, suggesting it might be related to money laundering or other criminal activities.
2. **Duration for Freezing an Account by BFIU:** According to the provisions mentioned:
 - The BFIU has the authority to issue an order to any reporting organization to **suspend or freeze transactions of any account**.
 - This suspension or freezing can be for a **maximum of 7 (seven) times**.
 - Each suspension or freezing period can last **up to 30 (thirty) days**.

These measures are part of the BFIU's efforts to combat money laundering and related financial crimes. The banks play a crucial role in this process by providing necessary information to the BFIU.

Q-19. Briefly explain the duties and responsibilities of Reporting Organizations.

Reporting organizations are required to fulfill specific duties and responsibilities to prevent money laundering, as outlined in Section 25(1) of the MLPA. These include:

1. Keeping accurate and complete information about the identities of their customers while their accounts are active.
2. After an account is closed, they must retain all records of that account and its transactions for at least five years.
3. They must provide information on customer identities and account transactions to the Bangladesh Financial Intelligence Unit (BFIU) upon request.
4. They are obliged to report any transactions or attempts of transactions that seem doubtful or suspicious as "suspicious transaction reports" to the BFIU immediately and proactively.

Q-20. How many Reporting Organizations (ROS) are there to report suspicious transaction to Bangladesh Financial Intelligence Unit (BFIU). Write the name of ROS. BPE-96th. BPE-98th. BPE-5th.

Bangladesh Financial Intelligence Unit (BFIU) recognizes 17 types of Reporting Organizations (ROs) for reporting suspicious transactions. These include:

1. Banks
2. Financial Institutions
3. Insurers
4. Money Changers
5. Companies or Institutions for remitting or transferring money
6. Institutions approved by Bangladesh Bank for business operations
7. Stock Dealers and Stock Brokers
8. Portfolio Managers and Merchant Bankers
9. Securities Custodians
10. Asset Managers
11. Non-Profit Organizations (NPOs)
12. Non-Government Organizations (NGOs)
13. Cooperative Societies
14. Real Estate Developers
15. Dealers in Precious Metals or Stones
16. Trust and Company Service Providers
17. Lawyers, Notaries, other Legal Professionals, and Accountants

Additionally, the BFIU has the authority to include any other institution as a reporting organization with government approval, ensuring a comprehensive network for monitoring and preventing suspicious financial activities.

Q-21. Write down the penalty provision for tipping off and providing false information to BFIU by a Reporting Organization (RO).

For providing false information to the Bangladesh Financial Intelligence Unit (BFIU), a Reporting Organization (RO) may face a fine ranging from Taka 20,000 to Taka 5 lacs. If fined more than three times in one financial year, BFIU can suspend or cancel the organization's registration or license, potentially leading to the closure of its operations within Bangladesh. Additionally, for non-compliance or knowingly submitting false information, the penalty can extend up to Taka 25 lacs, with Bangladesh Bank having the authority to suspend or cancel the license, requiring further action from the registering or licensing authority. Failure to pay fines allows Bangladesh Bank to recover dues by debiting the organization's accounts, and unresolved payments may lead to court involvement for recovery.

If a Reporting Organization (RO) provides false information to the Bangladesh Financial Intelligence

Unit (BFIU), the penalties are as follows:

1. The BFIU can impose a fine on the RO not less than Taka 20,000 but not exceeding Taka 5 lakhs.
2. If an RO is fined more than three times in a financial year, the BFIU may suspend the registration or license of the RO or its branches, service centers, booths, or agents, potentially leading to the closure of its operations in Bangladesh. The BFIU will also inform the registration or licensing authority for further action against the organization.

Furthermore, if an RO fails to comply with directions issued by Bangladesh Bank or knowingly provides false information:

1. The reporting agency can be fined by Bangladesh Bank up to Taka 25 lakhs.
2. Bangladesh Bank may suspend the registration or license of the agency or its operational units within Bangladesh and inform the relevant authorities for appropriate actions.
3. If the fine is not paid, Bangladesh Bank can recover the amount by debiting the RO's accounts in other banks or financial institutions, and if necessary, apply to the court for recovery of any unpaid amount.

Q-22. Describe the risk assessment framework of a bank as per ML/TF Risk Assessment Guideline issued by BFIU. BPE-97th.

The ML/TF Risk Assessment Framework for banks, as per the guidelines issued by the Bangladesh Financial Intelligence Unit (BFIU), is designed to ensure banks identify, assess, and effectively mitigate their risks related to money laundering (ML) and terrorist financing (TF). This framework is aligned with Recommendation 1 of the Financial Action Task Force (FATF), which mandates financial institutions and designated non-financial businesses and professions (DNFBPs) to proactively manage and control their ML/TF risks. According to Rule 10 of the Money Laundering Prevention Rules (MLPR) 2019, banks are required to conduct periodic risk assessments considering the nature of their business, products or services, countries of operation, and geographical locations. This process is crucial for establishing a robust anti-money laundering and combating the financing of terrorism (AML&CFT) regime within each financial institution, under the authority granted by the Money Laundering Prevention Act (MLPA), 2012, and the Anti-Terrorism Act (ATA), 2009, including their amendments.

Q-23. What is FATF? Write down 10 FATF recommendations.

The Financial Action Task Force (FATF) is an intergovernmental body established in 1989 by the Group of Seven (G-7) nations during their annual economic summit in Paris. Initiated with France as its first chair, FATF aims to lead global efforts against international money laundering. It has evolved from its initial G-7 framework to become the foremost entity providing Anti-Money Laundering (AML) guidance to governments worldwide. FATF's recommendations have significantly influenced global banking practices, legal frameworks, and governmental operations to combat money laundering and terrorism financing. The organization operates under the auspices of the Organization for Economic Cooperation and Development (OECD) in Paris, where it maintains its secretariat.

The FATF 40 Recommendations are a comprehensive set of guidelines for countries to combat money laundering and terrorist financing. Here are 10 of these recommendations:

1. Assess risks and apply a risk-based approach.
2. National cooperation and coordination.
3. Define money laundering offenses and confiscation measures.
4. Detail terrorist financing offenses and related sanctions.
5. Implement targeted financial sanctions related to terrorism and proliferation.
6. Ensure transparency and beneficial ownership of legal persons.
7. Strengthen the financial system and its regulation against ML/TF.
8. Enhance the role of law enforcement and operational measures.
9. Promote international cooperation and mutual legal assistance.
10. Require reporting entities to perform customer due diligence and record-keeping.

These recommendations aim to create a robust global framework to prevent, detect, and prosecute financial crimes and ensure international cooperation.

Q-24. What are the objectives of FATF?

The FATF's objectives include setting standards and promoting effective measures against money laundering, terrorist financing, and threats to financial integrity. It monitors members' progress on recommendations, reviews ML/TF techniques, and encourages global adoption of its standards. FATF assesses compliance and effectiveness, focusing on legal, institutional frameworks, and outcomes essential to robust AML/CFT systems. It aims for a coordinated global response, enhancing legal and operational measures and fostering international cooperation to combat financial crimes.

Q-25. What do you know FATF members and Observers? what do you understand by non-cooperative countries and territories (NCCTs)?

The Financial Action Task Force (FATF) consists of 37 member jurisdictions and 2 regional organizations, covering most major financial centers worldwide. It focuses on combating money laundering and terrorism financing. FATF has a history of "naming and shaming" countries with inadequate anti-money laundering controls through its Non-Cooperative Countries and Territories (NCCT) initiative. This effort aimed to identify jurisdictions with significant weaknesses in their anti-money laundering systems, using 25 criteria aligned with FATF's 40 Recommendations. The initiative led to the identification of 24 jurisdictions, pushing them to improve their systems. Nowadays, FATF continues to highlight jurisdictions with AML/CFT deficiencies, updating its findings thrice yearly in response to G-20 directives for identifying high-risk areas.

Non-Cooperative Countries and Territories (NCCTs) are jurisdictions identified by FATF as having inadequate anti-money laundering controls or not cooperating in global AML/CFT efforts. The NCCT process, initiated in 2000, aimed to reduce financial system vulnerability by ensuring all financial centers adopt internationally recognized measures against money laundering. Jurisdictions listed as NCCTs faced international pressure to reform their AML/CFT systems. This list has evolved into a process identifying jurisdictions with strategic deficiencies in their AML/CFT regimes, leading to regular updates on high-risk jurisdictions and those with strategic deficiencies to ensure global financial system protection.

Q-26. Define virtual asset (VA) and virtual asset service providers (VASPs) in line with FATF recommendation. BPE-96th. BPE-99th.

Virtual Assets (VAs) are digital representations of value that can be digitally traded or transferred and can be used for payment or investment purposes, excluding digital representations of fiat currencies.

Virtual Asset Service Providers (VASPs) are businesses or individuals that provide services related to one or more of the following: exchange between virtual assets and fiat currencies; exchange between one or more forms of virtual assets; transfer of virtual assets; safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset. These definitions align with FATF recommendations, emphasizing the need for countries and financial institutions to assess and mitigate the risks associated with VAs and VASPs, including their development, use, and the technologies that enable them.

Q-27. How VA and VASPS create ML & TF risk for banks and its customers? BPE-96th. BPE-99th.

Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs) introduce money laundering (ML) and terrorist financing (TF) risks to banks and their customers due to their inherent characteristics. The anonymity and global reach of VAs can obscure the origin of funds, making it challenging to identify and track illicit financial flows. VASPs, operating in a rapidly evolving digital landscape, may lack comprehensive regulatory oversight, allowing bad actors to exploit these platforms for ML/TF purposes. The speed and cross-border nature of transactions facilitated by VAs and VASPs complicate the monitoring and reporting processes, thereby increasing the risk exposure for financial institutions and their clientele to ML/TF activities. This scenario necessitates enhanced due diligence, continuous monitoring, and the development of sophisticated tools and practices by banks to effectively manage and mitigate these emerging risks.

Q-28. 'Digital transformation of financial system can reduce ML & 10 TF risk as well as it can create addition ML & TF risk' describe with some examples. BPE-96th. BPE-99th.

The digital transformation of the financial system can significantly impact the landscape of money laundering (ML) and terrorist financing (TF) risks. For instance, the adoption of digital identification and verification processes enhances the ability of financial institutions to accurately identify and verify customer identities, reducing the risk of fraudulent accounts and activities. Automated systems and machine learning algorithms can analyze vast amounts of transaction data in real-time, identifying suspicious patterns that may indicate ML or TF, thereby improving the detection and prevention capabilities of financial institutions.

Conversely, the same digital advancements also create new vulnerabilities. Cybercriminals can exploit digital platforms for the rapid movement of funds across borders, utilizing anonymity-enhancing technologies such as encrypted communications and cryptocurrencies to evade detection. Moreover, the pace of technological change can outstrip regulatory and law enforcement capabilities, leaving gaps that can be exploited for illicit purposes. This dual-edged nature of digital transformation underscores the need for continuous innovation in regulatory, compliance, and monitoring approaches to effectively manage the evolving risks associated with ML and TF in the digital age.

Q-29. Discuss about the FATF-Style Regional Bodies?

FATF-Style Regional Bodies (FSRBs) are essential components of the global network fighting money laundering (ML) and terrorist financing (TF). These regional bodies adhere to the standards set by the Financial Action Task Force (FATF) and work to implement these standards within their respective regions. FSRBs facilitate regional cooperation and coordination on AML/CFT efforts, providing a platform for sharing best practices, offering mutual assistance, and conducting peer reviews similar to FATF's mutual evaluation process. By tailoring the FATF recommendations to regional specifics, FSRBs ensure that countries within their jurisdiction can effectively address and mitigate the unique risks they face. This localized approach enhances the global fight against financial crimes by ensuring comprehensive coverage and allowing for targeted strategies that address regional nuances in ML/TF activities.

Q-30. What is APG? What Egmont Group? What are their functions in AML/CFT? BPE-99th.

The Asia/Pacific Group on Money Laundering (APG) is a FATF-style regional body (FSRB) that focuses on the Asia-Pacific region. It aims to combat money laundering (ML) and terrorist financing (TF) by promoting the adoption and implementation of international standards on

AML/CFT within its member jurisdictions. The APG facilitates regional cooperation, conducts mutual evaluations, and provides technical assistance and training to its members to strengthen their AML/CFT regimes.

The Egmont Group is an international organization comprised of financial intelligence units (FIUs) from around the world. It serves as a platform for the secure exchange of expertise and financial intelligence to combat ML and TF. The Egmont Group enhances international cooperation among its members by fostering better communication and collaboration, supporting the development of national FIUs, and promoting the effective implementation of AML/CFT measures globally.

Q-31. What are the benefits Bangladesh is getting as a member of Egmont Group? BPE-97th.

As a member of the Egmont Group, Bangladesh benefits significantly in enhancing its anti-money laundering (AML) and combating the financing of terrorism (CFT) efforts. Membership provides Bangladesh with access to a global network for the exchange of financial intelligence, crucial in tracing cross-border financial transactions related to ML and TF. It facilitates real-time information sharing among financial intelligence units (FIUs) worldwide, enabling Bangladesh to receive and provide valuable financial intelligence that supports the investigation and prosecution of money laundering and terrorist financing cases. Additionally, being part of the Egmont Group allows Bangladesh to leverage international expertise and best practices in AML/CFT, enhancing its capacity to establish more robust domestic financial monitoring and regulatory frameworks. This global cooperation strengthens Bangladesh's financial system against illicit financial flows and supports its efforts in maintaining international financial security.

Q-32. Write down the structure of Central and Divisional Taskforce.

The document provides detailed insights into the structure and functions of Divisional Taskforces in Bangladesh, particularly in combating money laundering and terrorist financing (AML/CFT). These taskforces coordinate with various law enforcement, regulatory authorities, and financial institutions to review and enhance divisional AML/CFT activities. Headed by office Heads of Bangladesh Bank's divisional offices, their membership includes representatives from diverse entities such as the Divisional Commissioner's office, Anti-Corruption Commission, Customs, Income Tax, Social Services, and various banks. Their main functions include coordinating with relevant agencies, reviewing progress on AML/CFT efforts, taking initiatives against barriers to AML/CFT implementation, and addressing issues like smuggling and trafficking.

Q-33. Which agencies are designated as investigative authorities for money laundering cases according to the Money Laundering Prevention Rules (MLPR), 2019 in Bangladesh?

According to the Money Laundering Prevention Rules (MLPR), 2019 in Bangladesh, several agencies are designated to investigate money laundering cases. These agencies can conduct investigations individually or jointly, depending on the related predicate offences. The specified investigative authorities are:

- Anti-Corruption Commission (ACC)
- Department of Narcotics Control (DNC)
- Criminal Investigation Department (CID), Bangladesh Police
- Bangladesh Securities and Exchange Commission (BSEC)
- Bangladesh Customs
- National Board of Revenue (NBR)

- Directorate of Environment

These agencies are empowered to investigate and address various aspects of money laundering activities within their respective domains.

Q-34. What is the establishment and nature of the Bangladesh Financial Intelligence Unit (BFIU) as per the Money Laundering Prevention Act (MLPA), 2012?

The Bangladesh Financial Intelligence Unit (BFIU) was established under Section 24 of the Money Laundering Prevention Act (MLPA), 2012. Originally formed as the Anti Money Laundering Department (AMLDD) in June 2002, it was renamed BFIU in 2012. The MLPA, 2012 ensures BFIU's operational autonomy, stating that it should have its own seal, letterhead, and office within the Bangladesh Bank premises. The Chief Officer of BFIU, appointed contractually by the government, has the status equivalent to that of a Deputy Governor of Bangladesh Bank. The BFIU is responsible for formulating and implementing policies on Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) with the government's approval and can request information and manpower from various government and law enforcement agencies.

Q-35. What are the penalties available for non-submission of STR/SAR? BPE-98th.

Penalties for non-submission of Suspicious Transaction Reports (STRs) or Suspicious Activity Reports (SARs) are significant to ensure compliance and prevent money laundering. The Bangladesh Financial Intelligence Unit (BFIU) can impose several penalties:

1. **Fines:** Organizations may face fines up to BDT 5 lakhs (500,000 Taka) at the rate of BDT 10,000 per day for each day of non-compliance. If fined more than three times in a financial year, the BFIU may suspend the organization's registration or license, effectively ceasing its operations within Bangladesh.
2. **Suspension of License:** Persistent non-compliance can lead to the suspension of the organization's registration or license, affecting its ability to conduct business
3. **Fines for False Information:** If false information or statements are provided, the organization can be fined between BDT 20,000 and 5 lakhs. Repeated offenses can also lead to license suspension
4. **Individual Penalties:** Responsible owners, directors, officers, and staff can also be fined between BDT 10,000 and 5 lakhs. Additionally, necessary administrative actions may be directed against them

Q-36. Department of Narcotic Control (DNC) request you to provide bank information of your customer. What kind of review you will do to response this request? BPE-99th.

When responding to a request from the Department of Narcotic Control (DNC) for customer bank information, the bank must follow strict compliance procedures and legal frameworks. The review process should include:

1. **Legal Compliance Review:** Verify if the request aligns with relevant laws, such as the **Money Laundering Prevention Act, 2012**, and **Banking Companies Act, 1991**. Customer information cannot be shared unless legally mandated.
2. **Regulatory Requirements:** Confirm if the request is approved by **Bangladesh Financial Intelligence Unit (BFIU)**, which is responsible for handling financial crime investigations.
3. **Court Order Validation:** Ensure that the request is backed by a valid court order or legal authorization from relevant authorities.

4. **Customer Due Diligence (CDD):** Check if the customer is involved in **Suspicious Transaction Reports (STRs)** or any flagged transactions related to **financial crime, money laundering, or drug trafficking**.
5. **Internal Review and Approval:** The compliance team should assess the risk, and senior management or the **Compliance Officer** should approve before sharing any information.
6. **Confidentiality and Data Protection:** Ensure that only the **minimum required information** is disclosed, following strict data privacy protocols.
7. **Record Keeping:** Maintain a record of the request, internal review, and response provided for future regulatory audits.

Only after ensuring legal and regulatory requirements are met should the bank proceed with responding to DNC.

Q-37. Investigating Authorities of Money Laundering Cases. BPE-99th.

Investigating Authorities of Money Laundering Cases

Money laundering cases can be investigated by one or more authorities depending on the nature of the related predicate offences. As per the **Money Laundering Prevention Rules (MLPR), 2019**, the following agencies are designated as investigating authorities:

1. **Anti-Corruption Commission (ACC)** – Investigates cases related to corruption and bribery.
2. **Department of Narcotics Control (DNC)** – Handles cases related to illegal drug and narcotics trade.
3. **Criminal Investigation Department (CID), Bangladesh Police** – Investigates various financial crimes, including counterfeiting, extortion, fraud, and organized crime.
4. **Bangladesh Securities and Exchange Commission (BSEC)** – Oversees cases of insider trading, market manipulation, and financial fraud in the capital markets.
5. **Bangladesh Customs** – Investigates smuggling and customs-related offences.
6. **National Board of Revenue (NBR)** – Handles tax-related offences and foreign currency trafficking.
7. **Directorate of Environment** – Investigates financial crimes related to environmental violations.

These authorities work jointly in cases where multiple offences overlap, ensuring a comprehensive approach to combating money laundering

Q-38. What is financial crime? Describe some common financial crime. BPE 5th .

Financial crime refers to illegal acts committed by individuals or organizations to gain financial or economic benefit. These crimes often involve money, property, or other assets and are usually carried out through deception, fraud, or abuse of position.

Example: A person creates a fake loan application and withdraws money from a bank account by providing false documents.

Here are some common financial crimes:

1. **Fraud:** Using lies or fake information to take money from banks, companies, or people.
2. **Money Laundering:** Hiding the source of illegal money by passing it through legal businesses or accounts.

3. **Bribery and Corruption:** Giving or taking money or gifts to get unfair advantages or decisions.
4. **Tax Evasion:** Not paying taxes by hiding income or giving false details to tax authorities.
5. **Identity Theft:** Using someone else's personal information to commit fraud or steal money.
6. **Insider Trading:** Using secret company information to make unfair profit from buying or selling shares.

These crimes are serious and hurt the economy and public trust.

Q-39. What are the penalties/sanctions available in MLPA for non performing of RO's responsibilities? BPE 5th

According to the Money Laundering Prevention Act (MLPA), if a Reporting Organization (RO) fails to perform its responsibilities, it may face several penalties or sanctions. These include:

1. **Financial Penalty** – The organization may be fined for non-compliance.
2. **Warning or Caution** – Bangladesh Financial Intelligence Unit (BFIU) may issue an official warning.
3. **Suspension or Cancellation** – License of the organization can be suspended or cancelled.
4. **Naming and Shaming** – Names of the defaulting organizations may be published in newspapers.
5. **Other Measures** – BFIU may take any other necessary action to ensure compliance.

These steps help enforce strong Anti-Money Laundering (AML) standards.

Q-40. During establishing business relationship, you have identified your potential customer is an Influential Person (IP) and his/her risk score is high. What due diligence measures you will take while establishing business relationship? BPE 5th.

Identifying the Customer as an Influential Person (IP)

If the potential customer is identified as an Influential Person (IP) and has a high-risk score, extra care must be taken. As per guidelines, IPs may include politicians, senior government officials, or individuals holding important positions in organizations.

Due Diligence Measures to be Taken

1. **Enhanced Due Diligence (EDD):** Collect additional information like income source, asset details, and financial background.
2. **Approval from Senior Management:** Before starting the relationship, take written approval from higher management.
3. **Close Monitoring:** Monitor the account more frequently to detect unusual or suspicious transactions.
4. **Ongoing Review:** Regularly update customer information and perform risk reviews.
5. **Screening:** Match the customer profile against sanction and watch lists.

Q-41. Detective Branch (DB) of Bangladesh police requested you to provide bank information of your customer. What kind of review you will do to response this request? BPE 5th.

When the Detective Branch (DB) of Bangladesh Police requests customer information, the bank must handle the request carefully. The following reviews should be done:

1. **Verify the Request Letter:** Check if the request is in writing and signed by an authorized officer from DB with official letterhead and seal.

2. **Legal Grounds:** Ensure that the request complies with applicable laws like the *Bankers' Book Evidence Act, 1891* or instructions from competent authorities.
3. **Internal Approval:** Get approval from the bank's legal and compliance department before sharing any customer information.
4. **Confidentiality Check:** Confirm that sharing information won't violate *Bank Secrecy* unless legally permitted.
5. **Record Keeping:** Keep records of the request and the response provided for future audit and compliance.

Q-42. While opening of a bank account of a company you identified that account owner of the company is holding 1% share and rest 99% is owned by a foreign firm. What kind of CDD measures you should follow in this case? BPE 5th.

When opening a bank account for a company where 99% is owned by a foreign firm and 1% by a local individual, the following Customer Due Diligence (CDD) measures should be taken:

1. **Identify Beneficial Owner:** Collect documents to confirm the foreign firm as the beneficial owner (owning 99%).
2. **Verify Foreign Entity:** Obtain registration certificate, business profile, and legal existence proof of the foreign firm.
3. **Check Ultimate Ownership:** Identify and verify the individuals who ultimately own/control the foreign firm.
4. **Screening:** Perform name screening of the foreign firm and its key persons against global watchlists.
5. **Risk Assessment:** Since a foreign entity is involved, consider it a higher risk and apply Enhanced Due Diligence (EDD).
6. **Source of Fund:** Collect declaration about source of funds and expected transaction profile.

Q-43. How you will identify beneficial owner of a company listed in capital market? BPE-5th

To identify the beneficial owner of a company listed in the capital market, follow these steps:

1. **Understand Ownership Structure:** Publicly listed companies usually have many shareholders.
2. **Look for Major Shareholders:** Check if any individual or entity owns or controls more than 5% or 10% of shares, depending on regulatory threshold.
3. **Review Disclosures:** Use stock exchange filings, company's annual reports, and public disclosures to identify major shareholders.
4. **No Single Owner:** In many cases, no single shareholder qualifies as a beneficial owner due to dispersed ownership.
5. **Apply Exceptions:** If no individual meets the ownership/control criteria, the company may not have a reportable beneficial owner under standard rules.
6. **Documentation:** Record findings and justification for no beneficial owner or list significant shareholders if required.

Q-44. How you will ensure 'complete and accurate' information of your customer? Explain with example. BPE 5th.

To ensure *complete and accurate* information of a customer, a bank should follow these steps:

1. **Use KYC Forms:** Collect all necessary details using a structured Know Your Customer (KYC) form.

2. **Verify Documents:** Match customer's provided data (name, address, ID number) with valid documents like NID, passport, or trade license.
3. **Cross-check Consistency:** Ensure the same spelling and number across all documents.
4. **Physical Verification:** Visit the address if required, especially for high-risk customers.
5. **Digital Checks:** Use verification tools or databases like NID Portal for checking national ID authenticity.
6. **Example:** If a customer writes their name as “Md. Rahim” in the form but NID says “Mohammad Rahim,” the correct one should be used based on the official ID.
7. **Documentation:** Keep copies of documents and record the verification steps.

Q-45. What are the responsibilities of Anti Money Laundering cell of your bank in submission of STR? BPE 5th.

Responsibilities of Anti Money Laundering (AML) Cell in Submission of STR:

1. **Receive Unusual Transaction Reports:** The AML cell collects reports from branches or departments that detect suspicious activity.
2. **Analyze Transactions:** It reviews the customer's profile, transaction pattern, and any unusual behavior.
3. **Conduct Internal Review:** The team evaluates the risk level and checks if the case meets the criteria of Suspicious Transaction Report (STR).
4. **Prepare STR:** If suspicious, the cell prepares a formal STR with all necessary facts and transaction records.
5. **Submit to BFIU:** The STR is submitted to Bangladesh Financial Intelligence Unit (BFIU) in the prescribed format through the goAML system.
6. **Maintain Confidentiality:** STRs must be kept confidential and never disclosed to the customer or unauthorized persons.

Q-46. What are the power and authority available for BFIU under the MLPA to make ROs compliant on AML & CFT? BPE 5th.

Power and Authority of BFIU under MLPA to Ensure RO's Compliance on AML & CFT:

1. **Monitoring Power:** BFIU can monitor and inspect if the Reporting Organization (RO) is following Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) laws.
2. **Information Collection:** BFIU can ask ROs to submit any documents or information needed for investigation.
3. **Issue Guidelines:** BFIU has the authority to issue circulars, instructions, or guidelines to ROs to improve compliance.
4. **Enforcement Action:** If any RO fails to comply, BFIU can impose administrative penalties like warnings, fines, or restrictions.
5. **Audit and Review:** BFIU can conduct audits or appoint inspectors to examine records related to AML/CFT compliance.

End of Module-A

অর্ডার করতে ক্লিক করুন: www.metamentorcenter.com

Or,

➡ WhatsApp: 01310474402