# OVERVIEW OF ORGANISATIONAL STRUCTURE IN INDIA FOR AML/CFT

## KYC/AML CHAPTER 7

Various laws have been enacted in India to address money laundering (ML) and terrorist financing (FT) concerns. A suitable organisational framework has also been devised and implemented for the effective enforcement of these laws. India is a member of the Financial Action Task Force (FATF) and several regional organisations. Overall coordination with these bodies falls under the **Ministry of Finance**. Measures related to terrorism, being matters of internal security, come under the purview of the **Ministry of Home Affairs**.

🔎 **Real-Time Example**

A recent FATF evaluation of a country can significantly impact its global financial reputation. For instance, if India undergoes an FATF assessment and achieves a favorable rating, it bolsters international confidence in its anti-money laundering and counter-financing of terrorism measures.

## ✨ 7.2 AML RELATED SET-UP

### 🌐 7.2.1 Ministry of Finance – FATF Cell

A dedicated **FATF Cell** under the Department of Economic Affairs in the Ministry of Finance is responsible for coordinating with the FATF and ensuring that India takes appropriate steps to implement FATF recommendations. This Cell manages tasks related to India's evaluation by the FATF and regional bodies concerning the Prevention of Money Laundering Act (PMLA). Its goal is to secure a high-level assessment for India, as such evaluations significantly influence the nation's standing in international financial markets.

### 🔎 Real-Time Example

After an on-site FATF evaluation, the FATF Cell might coordinate with various ministries and regulators to address any gaps found in India's AML/CFT framework. This proactive approach helps improve compliance and global perception.



### 🌐 7.2.2 Ministry of Finance – Financial Intelligence Unit – India (FIU-IND)

**Financial Intelligence Unit–India (FIU-IND)** serves as the central national agency for receiving, processing, analysing, and disseminating information on suspicious financial transactions to

enforcement agencies and foreign FIUs. It also coordinates and strengthens efforts among national and international intelligence, investigation, and enforcement agencies to combat money laundering and related crimes.

🔑 **Key Point**: The responsibility for ongoing implementation of FATF recommendations, especially those pertaining to money laundering, rests with FIU-IND.

**FIU-IND** was established by the Government of India (GOI) through an Office Memorandum dated 18 November 2004, under the Department of Revenue in the Ministry of Finance. It operates independently and reports to the Economic Intelligence Council (EIC), chaired by the Finance Minister. FIU-IND is considered the central pivot (fulcrum) of all AML-related activities in the country.

## 📜 7.2.2.1 Mission Statement and Organisation Vision

| Mission Statement | Organisation Vision |
|---|---|
| "To provide quality financial intelligence for safeguarding the financial system from the abuses of money laundering, terrorism financing and other economic offences." | "To become a highly agile and trusted organization that is globally recognized as an efficient and effective Financial Intelligence Unit." |

**Strategic Objectives** (to achieve the mission):

1. **Combat** Money Laundering, Financing of Terrorism, and other economic offences
2. **Deter** Money Laundering and Counter the Financing of Terrorism
3. **Build and strengthen** organisational capacity

**Thrust Areas** identified by FIU-IND:

- ⚙️ **Effective collection, analysis, and dissemination of information**
- 🤝 **Enhanced domestic and international cooperation**
- 📈 **Building capacity of reporting entities**
- ✅ **Ensuring compliance with reporting obligations under PMLA**
- 🏗️ **Building organisational resources**
- 💻 **Strengthening IT infrastructure**

🔎 **Real-Time Example**

To build capacity of reporting entities (e.g., banks or financial institutions), FIU-IND might conduct specialized workshops or training sessions on how to detect and report suspicious transactions. These sessions ensure that each entity fully understands its reporting obligations under PMLA.

## 📊 7.2.2.2 Functions of FIU-IND

FIU-IND primarily receives various transaction reports, analyses them, and disseminates pertinent financial intelligence to intelligence or law enforcement agencies (e.g., the Enforcement Directorate or Directorate of Revenue Intelligence).

| Function | Details |
|---|---|
| **(i) Collection of Information** | Acts as the central reception point for • Cash Transaction Reports (**CTRs**) • Cross Border Wire Transfer Reports (**CBWTRs**) • Suspicious Transaction Reports (**STRs**) • Reports on Purchase or Sale of Immovable Property (**IPRs**) |
| **(ii) Analysis of Information** | Evaluates data to identify patterns that suggest money laundering or related criminal activities. |
| **(iii) Sharing of Information** | Disseminates relevant intelligence to national intelligence/law enforcement agencies, national regulatory authorities, and foreign FIUs. |
| **(iv) Central Repository** | Maintains a national database on cash and suspicious transactions based on the reports received from reporting entities. |
| **(v) Coordination** | Strengthens the collection and exchange of financial intelligence via national, regional, and global networks to combat money laundering and related crimes. |
| **(vi) Research and Analysis** | Monitors and identifies strategic areas regarding money laundering trends, typologies, and emerging developments. |

🔎 **Real-Time Example**

Suppose a bank consistently files Suspicious Transaction Reports (STRs) about a particular account showing unusual patterns (e.g., multiple large deposits just below the CTR threshold). FIU-IND would analyze these STRs for possible money laundering indicators and share critical findings with relevant enforcement agencies.

## 💡 7.2.2.3 Initiatives of FIU-IND

In October 2012, FIU-IND launched its Information Technology system **FINnet** (accessible to reporting entities via the **FINgate** portal) for online submission of reports. FIU-IND utilizes **FINcore** to process these inputs. This system features robust data-linking capabilities, allowing all pertinent reports in the database to be connected using rules that resolve identities and relationships.

🔎 **Real-Time Example**

If a person under investigation for economic offences has multiple accounts across different banks, FINnet can link transactions from all those accounts, providing a comprehensive view of financial activity for further analysis.

📝 **SUMMARY TABLE**

Below is a concise overview of each section discussed:

| Section | Key Points |
|---|---|
| **7.1 Overview of Organisational Structure** | India has multiple laws addressing ML/FT. FATF coordination is handled by **Ministry of Finance**; terrorism matters fall under **Ministry of Home Affairs**. |
| **7.2.1 Ministry of Finance – FATF Cell** | A dedicated Cell oversees coordination with the FATF, managing evaluations under the PMLA and ensuring high-level assessments for India. |
| **7.2.2 FIU-IND** | Central agency for receiving, processing, and disseminating suspicious transaction information. Reports to EIC under the Finance Minister. |
| **Mission & Vision** | **Mission**: Provide quality financial intelligence **Vision**: Become a highly agile and globally recognized FIU. |
| **Functions of FIU-IND** | **Collection**, **Analysis**, **Sharing** of information; **Central Repository**, **Coordination**, **Research & Analysis**. |
| **Initiatives** | **FINnet** and **FINgate** portals for streamlined online reporting and robust data linking via **FINcore**. |

Below is the requested rewrite of Section **7.2.2.4 Processing/Sharing of Information** and **7.2.2.5 Measures for Improved Compliance with PMLA**, with added tables, real-time examples, and extensive use of emojis/icons. A summary table appears at the end. All original details have been preserved, and no new information has been added.

### ✨ 7.2.2.4 Processing/Sharing of Information

FIU-IND examines suspicious transactions not only on the basis of a single report but also by correlating all relevant information or reports—whether from other reporting entities or from cash transaction reports. This **value-added approach** ensures that information disseminated to partner agencies is more comprehensive and actionable.

### 🕵️ (i) Suspicious Transaction Reports (STRs)

FIU-IND receives, analyses, and disseminates STRs to various agencies. The number of STRs has shown an **increasing trend** over the years, attributed to continuous improvements in both the quality of reporting and focused attention on specific thrust areas.

### 🔎 Real-Time Example

A bank notices multiple large transactions with no apparent business rationale, possibly linked to an account previously flagged by another financial institution. FIU-IND combines these data points and disseminates them to enforcement agencies to investigate potential money laundering activities.

## Table 7.1 – Receipt of Suspicious Transaction Reports

| Reporting Entity Type | 2016-17 | 2017-18 | 2018-19 | 2019-20 | 2020-21 |
|---|---|---|---|---|---|
| **Banks** | 361,215 | 1,343,720 | 274,756 | 316,343 | 205,145 |
| **Financial Institutions** | 94,837 | 84,781 | 33,817 | 226,400 | N/A |
| **Intermediaries** | 16,954 | 7,839 | 14,589 | 4,270 | N/A |
| **Total** | 473,006 | 1,436,340 | 323,162 | 547,013 | 602,057 |

**Note**: Most STRs submitted relate to transactions characterized by unusual or unjustified complexity, or lacking an economic rationale or bonafide purpose.

### 🚚 Dissemination of STRs

FIU-IND decides **whether** to disseminate an STR and **which** agency should receive it based on:

- **Type of suspicion and nature of suspected offence**
- **Value and pattern of the transaction**, including linked reports
- **Linkage with other information**, including domestic agency data or foreign FIU inputs



## Table 7.2 – Dissemination of STRs

| Agencies | 2016-17 | 2017-18 | 2018-19 | 2019-20 | 2020-21 |
|---|---|---|---|---|---|
| **Law Enforcement Agencies** | 63,466 | 71,313 | 96,432 | 102,641 | 123,616 |
| **Intelligence Agencies** | 1,735 | 808 | 3,021 | 7,077 | 11,353 |
| **Regulators & Others** | 1,504 | 1,276 | 1,671 | 3,230 | 2,421 |
| **Total** | 156,978 | 65,022 | 76,920 | 66,170 | 137,390 |

**Note**:

- An STR may be disseminated to **more than one agency**.
- Therefore, totals may not match exactly across columns.
- For certain years, the total STRs disseminated to Law Enforcement Agencies exceed the aggregated total because of multiple-agency dissemination.

Since **large numbers** of STRs are filed by Reporting Entities (REs), FIU-IND prioritizes specific STRs tagged as **important** by REs. During FY 2019–20, **161** such STRs were prioritized, and in FY 2020–21, **979**. These STRs are handled by a dedicated "Important Cases Division" within FIU-IND.



## 💰 (ii) Cash Transaction Reports (CTRs)

Reports based on a **cash transaction threshold value** are a **major source** of information for FIU-IND and often help in linking with STRs, providing further investigative leads.

🔎 **Real-Time Example**

A public sector bank might file a CTR for repeated high-value cash deposits in a single week. FIU-IND then cross-references these deposits with any STRs submitted by other banks concerning the same individual or entity.



**Table 7.3 – Receipt of CTRs (2016–17 to 2020–21)**

| Reporting Entity Type | 2016-17 | 2017-18 | 2018-19 | 2019-20 | 2020-21 |
|---|---|---|---|---|---|
| Public Sector Banks | 10,40,667 | 87,74,954 | 84,31,594 | 96,85,711 | 77,82,519 |
| Indian Private Banks | 42,42,521 | 34,96,477 | 40,87,238 | 43,03,428 | 37,84,912 |
| Private Foreign Banks | 51,593 | 22,657 | 24,741 | 21,358 | 29,806 |
| Other Banks | 12,28,389 | 10,70,388 | 14,31,824 | 14,43,307 | 13,37,513 |
| Total | 1,59,29,176 | 1,33,64,476 | 1,39,75,397 | 1,54,59,804 | 1,29,34,750 |

**CTRs** are utilized for several purposes, including:

- Processing of STRs

- Handling requests for information from LEAs/IAs and **foreign FIUs**
- CTR analysis of **high-risk businesses** and **geographic locations**
- **Threshold analysis** (high-value transactions)
- Assisting in the **recovery of uncollected tax**
- **Matching Annual Information Report (AIR)** with CTR data to detect suspicious cash transactions around property purchases/sales
- Identifying **high-risk non-filers**, **stop filers**, and **defaulters** under Income Tax, GST, and Customs
- Investigating **financial crimes** reported in the media

### 🌏 (iii) Cross Border Wire Transfer Reports (CBWTRs)

CBWTRs cover cross-border wire transfers **exceeding ₹25 lakh** (or equivalent in foreign currency), where **either the origin or destination** of the funds is in India. These transfers may involve **any parties** and **any purpose**.



**Table 7.4 – Receipt of CBWTRs (2016–17 to 2020–21)**

| Year | Number |
|---|---|
| **2016-17** | 90,91,149 |
| **2017-18** | 94,07,903 |
| **2018-19** | 1,07,19,253 |
| **2019-20** | 3,95,53,003 |
| **2020-21** | 3,06,24,141 |

**Spike in Numbers**: In FY 2019–20, a strategic analysis revealed incomplete information in many CBWTR submissions. After guidance was issued, Reporting Entities **re-filed** many CBWTRs in FY 2020–21, causing the surge.

🔎 **Real-Time Example**

A high-value fund transfer from a foreign account to an Indian company catches FIU-IND's attention due to repeated round-tripping of funds. On analysis, FIU-IND disseminates the case to enforcement agencies for possible investigation into trade-based money laundering.



### 🤝 (iv) NPO Transaction Reports (NTRs)

NTRs apply to **all receipts** by Non-Profit Organizations (NPOs) exceeding ₹10 lakh.

**Table 7.5 – Receipt of NTRs (2016–17 to 2020–21)**

| Year | Number |
|---|---|
| **2016-17** | 6,78,786 |

| Year | Number |
|---|---|
| **2017-18** | 4,95,243 |
| **2018-19** | 4,39,412 |
| **2019-20** | 9,40,882 |
| **2020-21** | 7,91,307 |

### 🔎 Real-Time Example

An NPO receives multiple large foreign donations in a short period. FIU-IND may cross-check this against known high-risk channels or jurisdictions and alert relevant authorities if suspicious patterns emerge.

### 💵 (v) Counterfeit Currency Reports (CCRs)

Reporting entities must file CCRs for all cash transactions involving **forged or counterfeit currency** (or any forgery of a valuable security/document).

### Table 7.6 – Receipt of CCRs (2016–17 to 2020–21)

| Reporting Entity Type | 2016-17 | 2017-18 | 2018-19 | 2019-20 | 2020-21 |
|---|---|---|---|---|---|
| **Public Sector Banks** | 1,01,167 | 60,768 | 32,347 | 25,476 | 15,960 |
| **Indian Private Banks** | 5,92,677 | 2,52,213 | 2,64,223 | 2,26,469 | 1,63,752 |
| **Private Foreign Banks** | 14,361 | 2,127 | 1,466 | 1,054 | 681 |
| **Other Banks** | 6,930 | 25,303 | 38,687 | 9,165 | 7,791 |
| **Total** | 7,33,508 | 3,53,795 | 3,31,682 | 2,62,164 | 1,88,184 |

**Source**: Annual Report (2020–21), FIU-India

## ✨ 7.2.2.5 Measures for Improved Compliance with PMLA

One of FIU-IND's key functions is ensuring that reporting entities **comply** with the obligations under PMLA. FIU-IND employs a **multi-pronged strategy** comprising the following:

1. **Increasing awareness for voluntary compliance**
    - Outreach programs with regulators and industry associations
    - Encouraging professional institutes to offer AML/CFT courses
    - Internal training for employees of reporting entities
    - Highlighting high-risk scenarios
2. **Regular review meetings for ensuring reporting**
    - Sector-specific meetings in coordination with the regulator
    - Individual meetings with entities needing additional guidance
    - Sensitizing senior management in reporting entities
    - Providing regular quality feedback
3. **Detecting contraventions in reporting**

- Obtaining information on PMLA violations from Law Enforcement Agencies
- Checking if all connected reporting entities have filed required reports
- Identifying entities needing detailed reviews or on-site inspections

4. **Imposing sanctions where necessary**
   - Allowing time for entities to rectify mistakes
   - Issuing warnings and advising corrective measures
   - Imposing fines for continued or serious contraventions
   - Monitoring for 6–12 months post-sanction
5. **Enforcement actions (2019–20 and 2020–21)**
   - In FY 2019–20: Show cause notices issued to **82** entities; **17** orders issued imposing fines of **₹19.46 crore**
   - In FY 2020–21: **27** show cause notices; **17** penalty orders imposing fines of **₹1.5 crore**
6. **Project FINnet 2.0**
   - Advanced capabilities and upgraded features to improve data processing
7. **Learning Management System (LMS)**
   - Launched for staff of regulators and reporting entities (registered on FINnet 2.0)
8. **Development of Red Flag Indicators**

- Sector-specific red flags to assist with STR detection and reporting
- Guidance includes high-risk customers, products, services, and geographies
- Common alerts for suspicious transaction detection and STR preparation

9. **Guidance Notes Issued by FIU**
   - Detecting suspicious TBML transactions (2015)
   - Effective STR detection/reporting for co-operative banks (2016)
   - Effective STR detection/reporting for scheduled commercial banks (2017/2018)
   - Guidelines on detecting STRs related to Terror Financing/NGOs/FICN (2018)
   - Guidelines on detecting STRs linked to finance components of Afghan drug business (2018)
10. **Strategic Analysis Lab (SAL)**
    - A specialized group focused on research in AML and fostering innovation in this domain

## 📝 SUMMARY TABLE

| Section | Key Takeaways |
|---|---|
| **7.2.2.4 – Processing/Sharing of Information** | FIU-IND correlates various reports (STRs, CTRs, etc.) for enhanced accuracy before disseminating information. STR numbers have risen, and FIU-IND prioritizes STRs flagged as important. |
| **Suspicious Transaction Reports (STRs)** | Large increases over time; disseminated to multiple agencies. Certain STRs undergo fast-track analysis by an Important Cases Division. |
| **Cash Transaction Reports (CTRs)** | Cover high-value cash dealings. Used for investigating high-risk businesses, threshold analysis, tax evasion tracking, and more. |
| **Cross Border Wire Transfer Reports (CBWTRs)** | Involve transfers over ₹25 lakh. Re-filing caused recent surges. Critical for detecting round-tripping and foreign remittances with possible laundering risks. |
| **NPO Transaction Reports (NTRs)** | Reports any non-profit receipts above ₹10 lakh. Helps detect questionable foreign or domestic donations. |
| **Counterfeit Currency Reports (CCRs)** | Mandatory for forged/counterfeit currency usage or document forgery. Numbers have varied due to demonetization and enhanced detection. |
| **7.2.2.5 – Measures for Improved Compliance** | **Multi-pronged strategy**: (1) Awareness & outreach (2) Review meetings (3) Detection of contraventions (4) Sanctions (5) Technology upgrades (FINnet 2.0, LMS) (6) Red Flag Indicators & Guidance notes (7) Strategic Analysis Lab for AML research. |

Below is a **rewritten** version of **Sections 7.2.3, 7.2.4, and 7.3**, featuring **extensive emojis/icons** for enhanced readability and visual appeal. **All original information, meaning, and structure remain unchanged**, and no additional details have been introduced.

## 🌟 7.2.3 Directorate of Enforcement (ED)

The **Directorate of Enforcement (ED)** was established in **1956** and is responsible for enforcing:

- The **Foreign Exchange Regulation Act (FERA), 1973** (prior to its repeal).
- The **Foreign Exchange Management Act (FEMA), 1999** (currently in force).

Following the enactment of the **Prevention of Money Laundering Act (PMLA), 2002**, certain provisions of that law were also entrusted to the ED. **ED** functions under the **Department of Revenue**.

### 🔍 Real-Time Example

If a firm is suspected of running a “hawala” network by illegally transferring foreign currency without proper records, the ED would gather intelligence, investigate potential FEMA violations, and initiate legal proceedings under relevant PMLA provisions if required.

## ⚙️ Main Functions of ED

| ⚡ Function | 💡 Details |
|---|---|
| **1 Collect, develop & disseminate intelligence** | Gathers information on activities that could breach FEMA (e.g., unauthorized foreign exchange dealings). |
| **2 Investigate suspected violations** | Probes issues like **"hawala,"** foreign exchange racketeering, non-realization of export proceeds, or non-repatriation of foreign exchange under FEMA. |
| **3 Adjudicate cases under FERA/FEMA** | Conducts legal proceedings for violations under **FERA, 1973** (before its repeal) and **FEMA, 1999**. |
| **4 Process COFEPOSA cases** | Handles preventive detention under the **Conservation of Foreign Exchange and Prevention of Smuggling Activities Act (COFEPOSA)**. |
| **5 PMLA enforcement** | Carries out surveys, searches, seizures, arrests, and prosecutions for **PMLA** offenses. |

## 🌟 7.2.4 Serious Frauds Investigation Office (SIFO)

The **Serious Frauds Investigation Office (SIFO)** operates under the **Ministry of Corporate Affairs**. It investigates and prosecutes (or recommends prosecution for) **white-collar crimes/frauds**, supported by a multi-disciplinary team of experts in:

- 🏦 **Accountancy**
- 🔎 **Forensic auditing**
- ⚖️ **Law**
- 💻 **Information technology**
- 🔬 **Investigation**

- 🏢 **Company law**
- 📈 **Capital markets**
- 💰 **Taxation**

🔍 **Real-Time Example**

When a large conglomerate is alleged to have falsified financial statements and siphoned off investor funds, **SIFO** may be directed to investigate. Its forensic team would analyze transactions, uncover complex money trails, and recommend legal action.

🏢 **Key Criteria for SIFO Investigations**

- **Complexity** requiring **inter-departmental** and **multi-disciplinary** intervention
- **Substantial public interest**, judged by either the **monetary scale** of misappropriation or the **number of affected persons**
- Potential for investigation to foster **systemic improvements** in **laws**, **procedures**, or **regulatory frameworks**

**Note**: SIFO handles serious fraud cases referred by the **Department of Company Affairs**.



## 🌟 7.3 CFT RELATED SET-UP – NATIONAL INVESTIGATION AGENCY (NIA)

India has been a **victim of terrorism** for many years, experiencing attacks ranging from:

- Militancy/insurgency in certain regions
- Left-Wing Extremism
- Bombings and terror incidents in major cities or other areas

These episodes often involve **complex inter-State** and **international** dimensions, including:

- 🚫 **Smuggling of arms** and **drugs**
- 💸 **Circulation of counterfeit Indian currency**
- 🚧 **Cross-border infiltration**

🔍 **Real-Time Example**

A bomb blast in a major city potentially funded by overseas terror networks would typically be investigated by the **NIA**, which collaborates with state police and intelligence agencies to track the funding and support channels.

## 🌐 Mandate of NIA

Established under the **National Investigation Agency Act, 2008**, the **NIA** serves as **India's Central Counter Terrorism Law Enforcement Agency**. It investigates and prosecutes offenses that impact:

- The **sovereignty, security, and integrity** of India
- **Friendly relations** with foreign states
- Violations under laws implementing **international treaties**, **UN resolutions**, and other global conventions

In essence, the **NIA** targets crimes and terrorist activities with **national ramifications**.

## 📝 SUMMARY TABLE

| 📑 Section | 🔑 Focus | ✔️ Key Points |
|---|---|---|
| **7.2.3 – ED** | Enforcement of **FEMA** & specific **PMLA** provisions | **Established 1956**. Investigates foreign exchange violations (e.g., hawala), adjudicates FERA/FEMA offenses, and processes detention cases under COFEPOSA. |
| **7.2.4 – SIFO** | Investigation of **white-collar crimes/frauds** in corporate sector | **Multi-disciplinary** team of experts. Handles serious frauds with significant monetary or public impact, often referred by the **Department of Company Affairs**. |
| **7.3 – NIA** | **Counter Terrorism** operations, investigations, and prosecutions | **Set up under NIA Act, 2008**. Investigates crimes affecting India's sovereignty/security, including terrorist activities potentially linked to global finance networks. |



**All original details, structure, and intent have been retained. Emojis and icons are included extensively for improved aesthetic appeal and readability.**

Below is a **rewritten** version of **Sections 7.4, 7.5, and 7.6**, making **extensive use of emojis and icons** to enhance visual appeal. The **original meaning, structure, and details** remain intact, with **no**

**additional or omitted information**. A **summary table** appears at the end, and **real-time examples** have been included for clarity.

## 🌟 7.4 NATIONAL ML/TF RISK ASSESSMENT SET-UP

In line with the **Risk-Based Approach** (RBA) adopted for the **FATF Standards of 2012**, the FATF issued a **Guidance Document** on **National AML/CFT Risk Assessment** in **2013**. Consequently, an **AML Steering Committee (AML-SC)** was formed under the **Department of Revenue, Ministry of Finance** in **February 2012** to oversee India's National Risk Assessment efforts.

### 🔍 Terms of Reference of the AML-SC

1. **Periodic Assessment of ML Risks**
    - Evaluate **financial products and services**, financial sectors, and geographical jurisdictions.
2. **Objective Assessment of PMLA Implementation**
    - Measure effectiveness, identify **legislative** or **administrative** gaps.

### 🤝 Agencies & Departments Involved in National Risk Assessment

1. **Department of Revenue**
2. **Department of Economic Affairs (DEA)**
3. **Enforcement Directorate (ED)**
4. **Financial Intelligence Unit-India (FIU-IND)**

5. **Central Board of Direct Taxes (CBDT)**
6. **Directorate General of Revenue Intelligence (DGRI)**
7. **Directorate General of Central Excise Intelligence**
8. **Directorate General of Foreign Trade**
9. **Serious Frauds Investigation Office (SFIO)**
10. **Reserve Bank of India (RBI)**
11. **Securities and Exchange Board of India (SEBI)**
12. **Insurance Regulatory and Development Authority (IRDA)**

🔎 **Real-Time Example**

A potential money laundering scheme might span multiple sectors—banking, insurance, and foreign trade. The AML-SC ensures that each relevant agency collaborates to assess risks holistically, from **account deposits** to **trade-based** transactions.



🏦 **Sector-Specific Working Groups (SWGs)**

During **2013-14**, SWGs for the **banking**, **insurance**, and **capital market** sectors were established under their respective regulators' chairmanship. These groups include representatives from:

- Law Enforcement Agencies (LEAs)
- Regulators
- FIU
- Industry

## 🌐 National Risk Assessment Working Group (WG)

In **August 2015**, the Government formed a **Working Group (WG)** of key agencies to conduct a **National Risk Assessment** of various sectors, using **World Bank methodology**. The WG is supported by **eight teams**, each responsible for areas like:

- **Terrorist Financing Threat**
- **Terrorist Financing Vulnerability**
- **Banking Sector**
- **Insurance Sector**
- **Capital Market**
- **Other Financial Institutions**
- **NFPBs** and **Financial Inclusion**

Besides the **Department of Revenue**, other participants include:

- **Ministry of Home Affairs**
- **Ministry of Corporate Affairs**
- **Income Tax Department**
- **Financial Intelligence Unit (FIU)**
- **National Investigation Agency (NIA)**
- **RBI**, **SEBI**, **IRDAI**

## 🌟 7.5 ASSOCIATION WITH INTERNATIONAL/REGIONAL BODIES

India is actively involved with several **international agencies** in the **AML/CFT** domain:

1. **FATF**
    - Initially an **observer**. Became a **member** on **June 25, 2010**.
2. **Eurasian Group (EAG)**
    - Joined as an observer. Achieved **membership** in **December 2010**.
3. **Asia/Pacific Group on Money Laundering (APG)**
    - Member since **March 1998**. Served as **co-chair (2010–12)**.
    - FIU-IND contributes an **expert** to the **Mutual Evaluation Working Group (MEWG)** of APG.
4. **Egmont Group**
    - FIU-IND joined in **May 2007**.
    - Serves as one of **two regional representatives** for Asia, alongside Qatar.
    - Actively participates in Working Groups: **Membership Support & Compliance (MSCWG)**, **Information Exchange (IEWG)**, and **Policy & Procedure (PPWG)**.
5. **BIMSTEC Sub-Group on Combating Financing of Terrorism**
    - FIU-IND represents India in this forum addressing **terrorism financing** across **South Asia** and **South East Asia**.

### 🔎 Real-Time Example

A suspicious transaction flagged in India could link to a shell company overseas. Through APG or Egmont Group channels, FIU-IND collaborates with foreign FIUs to gather additional intelligence and expedite investigations.

## 🌟 7.6 INTERNATIONAL CO-OPERATION/BILATERAL AGREEMENTS

**FIU-IND** may exchange information with **foreign FIUs** on a **reciprocal basis**, without requiring a formal **Memorandum of Understanding (MoU)**. Nevertheless, to **strengthen cooperation** and establish a **structured framework**, FIU-IND has signed **bilateral MoUs** with several FIUs of countries with significant commercial ties to India.



### 📊 Table 7.7 – Exchange of Information with Foreign FIUs

| Status of Action Taken | 2016-17 | 2017-18 | 2018-19 | 2019-20 | 2020-21 |
|---|---|---|---|---|---|
| Requests Received from Foreign FIUs | 123 | 109 | 111 | 135 | 137 |
| Requests Sent to Foreign FIUs | 138 | 177 | 288 | 485 | 405 |
| Spontaneous Referrals Received from Foreign FIUs | 125 | 129 | 160 | 180 | 209 |

**Source**: Annual Report (2020–21), FIU-India

### 🔎 Real-Time Example

If an overseas FIU uncovers a lead involving Indian individuals, it may **spontaneously refer** the case to FIU-IND. Conversely, FIU-IND can request foreign FIUs to help track money flows or assets located abroad.

### 🔗 Other Collaborative Efforts

- FIU-IND participates in the **India-Russia-USA Trilateral Working Group** on **financial aspects of Afghan drug trade**, sharing information on **drug-related offenses**.
- FIU-IND has provided **technical assistance** to **FIU-Bhutan** for setting up an electronic reporting system; relevant hardware was supplied to them.
- FIU-IND also joins the **Joint Working Groups (JWGs) on Counter Terrorism**, which the Government of India has established with various countries. These JWGs evaluate **AML/CFT vulnerabilities** and **national risk assessments**.



### 📝 SUMMARY TABLE

| 📑 Section | 🔎 Focus | ✔️ Key Points |
|---|---|---|
| **7.4 – National ML/TF Risk Assessment Set-Up** | **Risk-Based Approach**, AML Steering Committee, NRA Working Groups | India applies **FATF** guidance for risk assessment. AML-SC formed to periodically assess ML/TF risks. |

| 📑 Section | 🔎 Focus | ✔️ Key Points |
|---|---|---|
| | | Sectoral WGs for banking, insurance, capital markets. |
| **7.5 – Association with International Bodies** | India's involvement with **FATF**, **EAG**, **APG**, **Egmont Group**, **BIMSTEC** | Became an FATF member in **2010**; APG co-chair (2010–12); Egmont Group member since **2007**; multi-forum collaboration on AML/CFT. |
| **7.6 – International Cooperation & Bilateral** | Information exchange with **foreign FIUs** and **technical assistance** | FIU-IND can share info on a **reciprocal basis** without an MoU but also signs bilateral MoUs. Engaged in **Trilateral Working Groups** and **JWGs** on counter-terrorism. |



**All essential details have been preserved, while emojis/icons and real-time examples have been added to enhance visual appeal and comprehension.**

Below is a **rewritten** version of **Section 7.7** with **extensive emojis/icons** for better readability and a **summary table** at the end. The **original meaning, structure, and details** remain **unchanged**, and **no new information** has been added.

## 🌟 7.7 SOME PENAL ACTIONS BY FIU-INDIA

FIU-IND, in line with its obligations under the **Prevention of Money Laundering Act (PMLA)**, monitors Reporting Entities (REs) for compliance. In cases of **serious or significant non-compliance**, FIU-IND may **levy monetary penalties** or take other **penal measures**. Below are examples of such actions:

### 🏦 (a) Order of 29th July 2019

💰 **Penalty: ₹15,62,90,000/-**

⚠️ **Non-Compliance Issues**

- ❌ **Failure** to file certain **threshold-based reports**
- ❌ **Failure** to file certain threshold-based reports **accurately** and/or **within the prescribed timeline**
- ❌ **Failure** to file **suspicious transaction reports (STRs) timely** and **accurately**
- ❌ **Failure** to implement an **effective internal mechanism** for threshold-based and suspicious transaction reporting
- ❌ **Failure** to submit **correct data** to FIU-IND

### 🔔 Penal Action: Warning Issued

⚠️ **Non-Compliance Issues**

- ❌ **Failure** to identify and verify **beneficial owners** in several customer accounts

- ❌ **Failure** of the system to detect **multiple transactions just below the threshold** for walk-in customers
- ❌ **Failure** to conduct **risk assessment** related to money laundering and terrorist financing risks (covering products, services, delivery channels, or locations)
- ❌ **Failure** to **fully implement** a Client Due Diligence (CDD) programme, particularly regarding **beneficial ownership** details and **risk assessment**

### 🏦 (b) Order of 19th March 2019

💰 **Penalty: ₹23,00,000/-**

⚠️ **Non-Compliance Issues**

- ❌ **Failure** to maintain an **effective mechanism** for detecting **all suspicious transactions**
- ❌ **Failure** to identify and verify the **ultimate beneficial owner** for trusts, legal entities, and similar customers
- ❌ **Failure** to **fully implement** a CDD programme, especially regarding screening against the **latest UNSC sanctions list**

### 💬 Observations

"...it would be worthwhile to state that xxxxxx is one of the oldest public sector banks and as such it must act as a torchbearer of the AML compliance in the country. Given the fact that the Bank is at the

forefront of banking operations in India, the Bank does not have any dearth of resources or capacity for statutory compliances in respect of AML. I also note that the Bank has claimed to have taken several remedial measures to improve its AML systems.

However, considering that the non-compliances, as enumerated above, were continuing till pointed out during the review by FIU-IND despite statutory obligations and keeping in mind that the penalty for the said failures and non-compliance has to be effective, proportionate and dissuasive... impose a monetary penalty on the Bank in the manner as detailed below in the table."



🏦 **(c) Order of 27th March 2018**

💰 **Penalty: ₹29,00,00,000/-**

⚠️ **Non-Compliance Issues**

- ❌ **Failure** to maintain an **effective internal system** for disposing of alerts and for detecting/reporting suspicious transactions
- ❌ **Failure** in **customer due diligence** for certain accounts
- ❌ **Delayed filing** of certain **Electronic Fund Transfer** reports

- ❌ **Failure** to file Electronic Transfer Reports in specific accounts
- ❌ **Non-filing** of integrally connected CRs in certain accounts
- ❌ **Not filing** STRs in certain new accounts belonging to one family, despite numerous CTRs
- ❌ **Improper STRs** in some accounts and **delayed filing** in others

## 💬 Observations

"...The question that the Bank should ask itself is – does the policy and procedure adopted by the Bank ensure effective compliance with the requirements of the provisions of the Act and the Rules thereunder?

Does it ensure integrity of the financial system in the face of growing malaise of money laundering?

Does it have the ability to timely detect and thwart [transactions] that have potential of money laundering and terror financing? The answer to all these questions is no.

Considering that these failures were deliberate and willful and keeping in mind that the interdiction for the said failures and non-compliance has to be effective, proportionate and dissuasive, I... hereby impose monetary penalty on the Bank in the manner as detailed below in the table."

## 📝 SUMMARY TABLE

| Date of Order | Penalty | Key Non-Compliance Highlights |
|---|---|---|
| **29th July 2019** | ₹15,62,90,000 | - Delayed/inaccurate threshold & STR reporting - Inadequate internal mechanisms - Incorrect data submission |
| **(Same Order)** Warning | *Warning Issued* | - Failure to identify beneficial owners - No risk assessment mechanism - No systems for repeated small transactions |
| **19th March 2019** | ₹23,00,000 | - Ineffective detection of suspicious transactions - Poor beneficial ownership verification - Weak UNSC sanctions screening |
| **27th March 2018** | ₹29,00,00,000 | - Weak internal systems for alerts/STR - CDD failures - Delayed/non-filed EFT reports - Improper STRs |