

**AML Policy**  
**Globe Capital (IFSC) Limited**

**Approved by Board on 11-Feb-2025**

## **Introduction of Globe Capital (IFSC) Limited**

Globe Capital (IFSC) Limited is a member of India International Exchange IFSC (INDIA INX), NSE IFSC Limited and India International Bullion Exchange (IIBX) having SEBI/ IFSCA registration no. INZ000097337.

This Anti-Money-Laundering (AML) policy has been prepared in accordance with IFSCA guidelines & circulars and Prevention of Money Laundering Act, 2002 (PMLA Act).

## **CHAPTER-1**

### **OVERVIEW**

#### **1.1 Introduction and Background of AML**

International Financial Services Centres Authority (IFSCA) issues necessary directives related to Anti-Money Laundering (AML), Client Due Diligence (CDD) and Combating Financing of Terrorism (CFT) as and when required.

The guidelines given by IFSCA are intended for the use primarily by intermediaries registered. The overriding principle is that the intermediaries should be able to satisfy themselves that the measures taken by them are adequate, appropriate and abide by the spirit of such measures and the requirements as enshrined in the PMLA.

The provisions of the Guidelines shall apply to every Regulated Entity which is licensed, recognised or registered by International Financial Services Centres Authority (IFSCA) and also to the Regulated Entities authorised by it, to the extent specified. The provisions of these Guidelines shall also apply to a Financial Group of the Regulated Entity, to such extent as specified in Chapter-XII. Every regulated entity have to adhere to client account opening procedure and maintain a record of all such transactions; the nature and value of which has been prescribed in the Rules notified under the PMLA. Such transactions include:

- a) All cash transactions of the value of more than Rs 10 lakhs or its equivalent in foreign currency.
- b) All series of cash transactions integrally connected to each other which have been valued below Rs 10 lakhs or its equivalent in foreign currency where such series of transactions take place within one calendar month and the aggregate value of such transactions exceeds rupees ten lakh;
- c) All suspicious transactions whether or not made in cash and including inter-alia credits or debits into from any non monetary account such as demat account, security account maintained.

It may, however, be clarified that for the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related ' shall also be considered

## **1.2 Policies and procedures to combat Money Laundering and Terrorist Financing**

### **1.2.1 Obligation to establish policies and procedures:-**

- a) Global measures taken to combat drug trafficking, terrorism and other organized and serious crimes have all emphasized the need for financial institutions, including securities market intermediaries, to establish internal procedures that effectively serve to prevent and impede money laundering and terrorist financing. The PMLA is in line with these measures and mandates that all reporting entities ensure the fulfillment of the aforementioned obligations.
- b) To be in compliance with these obligations, the senior management of a registered entity shall be fully committed to establishing appropriate policies and procedures for the prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. The Registered entity shall :-
  - i) issue a statement of policies and procedures, where applicable, for dealing with ML and TF reflecting the current statutory and regulatory requirements;
  - ii) ensure that the content of these Directives are understood by all staff members;
  - iii) regularly review the policies and procedure to ensure their effectiveness;
  - iv) adopt client acceptance policies and procedures
  - v) undertake client due diligence (CDD) measures to an extent that is sensitive to the risk of ML and TF depending on the type of client , business relationship or transaction;
  - vi) have system in place for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities
  - vii) develop staff members awareness and vigilance to guard against ML and TF;

**1.2.2 Policies and procedures to combat ML shall cover:-**

- a) Communication of company policies relating to prevention of ML and TF to all management and relevant staff;
- b) Client acceptance policy and client due diligence measures;
- c) Maintenance of records;
- d) Compliance with relevant statutory and regulatory requirements;
- e) Co-operation with the relevant law enforcement authorities including timely disclosure of information;
- f) Role of internal audit or compliance function to ensure compliance with the policies, procedures and controls relating to the prevention of ML and TF. The Internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure and number of clients and other such factors.

**CHAPTER-2****DETAILED DIRECTIVES****2.1 Vision towards Anti Money Laundering**

- 2.1.1 Globe Capital (IFSC) Limited has resolved that it would, as an internal policy, take adequate measures to prevent money laundering and shall put in place a frame-work to report suspicious transactions to FIU as per the guidelines of PMLA Rules, 2002 and as prescribed by IFSCA in its Guidelines.
- 2.1.2 For suspicious transactions whether or not made in cash, we observe the trading pattern of the client on difference criteria like market participation, Income & Networth, funds received, trading behaviour etc.
- 2.1.3 Compliance department of company review & update AML policy on time to time based on the guidelines issued by regulator in consultation with Principal Officer.

**CHAPTER-3****CUSTOMER DUE DILIGENCE**

**3.1.** After assigning risk rating for each Customer proportionate to their AML/CFT risks, shall undertake the Customer Due Diligence. While undertaking the CDD, we: -

- (i) undertake Customer Due Diligence measures as detailed under Clause 3.4, in respect of all the customers;
- (ii) undertake Enhanced Customer Due Diligence measures as detailed under Clause 3.6, in addition to the CDD measures detailed under Clause 3.4, in respect of the customer who has been assigned 'high risk'; and,
- (iii) Undertake Simplified Customer Due Diligence measures as detailed under Clause 3.7 by modifying Customer Due Diligence process detailed under Clause 3.4, in respect of a customer who has been assigned 'low risk'.

**3.2. Timing of CDD**

- (a) Except as otherwise provided in Clause 3.3 and 3.4, we shall undertake the Customer Due Diligence of a customer: -
  - (i) at the time of establishing business relationship, as mandated under Clause 3.4.1 (a) to (c); and,
  - (ii) after establishing a business relationship, as mandated under Clause 3.4.1.(d).
- (b) We shall also undertake Customer Due Diligence if, at any time:
  - (i) in relation to an existing customer, it doubts the veracity or adequacy of documents, data or information obtained for the purposes of Customer Due Diligence;
  - (iii) it suspects ML/TF; or,
  - (iii) there is a change in risk-rating of the customer, or it is otherwise warranted by a material change in circumstances of the customer.

**3.3. Establishing business relationship before verification**

- (a) We may establish a business relationship with a customer before completing the verification required under Clause 3.4.1, subject to fulfilling the following conditions:
  - (i) the deferral of completion of the verification of the customer or Beneficial Owner is essential in order not to interrupt the normal conduct of a business relationship;

- (ii) there is low risk of occurrence of ML/TF activity and any such risks identified can be effectively managed by us;
  - (iii) in relation to a bank account opening, there are adequate safeguards in place to ensure that the account is not closed, and transactions are not carried out by or on behalf of the account holder (including any payment from the account to the account holder) before verification has been completed; and
  - (iv) subject to Clause 3.3 (b) below, the relevant verification is completed as soon as reasonably practicable and, in any event, it should not exceed 30 business days after the establishment of business relationship.
- (b) Where we are not able to comply with the 30-day requirement, it shall, prior to the end of the 30-day period:
  - (i) document the reason for its non-compliance;
  - (ii) complete the verification as soon as possible; and
  - (iii) record the non-compliance event for reporting to its Governing Body.
- (c) We shall suspend business relationship with the customer and refrain from carrying out further transactions (except to return funds to their sources, to the extent that is possible) if such verification remains uncompleted for 30 days after the establishment of business relationship.
- (d) We shall terminate business relations with the customer if such verification remains uncompleted for 120 days after the establishment of business relationship.

### **3.4. Customer Due Diligence Requirements**

#### **3.4.1. Undertaking Customer Due Diligence (CDD)**

In undertaking Customer Due Diligence as required under Clause 3.1.(a) (i), the following measures shall be undertaken: -

- (a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.
- (b) Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, in such a manner that we are satisfied that it knows who the beneficial owner is. Similarly, for legal persons and arrangements, the CDD shall include taking reasonable steps to understand the nature of the customer's business, its ownership and control structure.

- (c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.
- (d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of business relationship to ensure that the transactions that are being conducted, are consistent with our knowledge of the customer, customer's business and risk profile, including, where necessary, the source of funds.

### **3.4.2. Identification of Customer**

- (a) If a customer is a natural person, we shall obtain at least the following information:
  - (i) Full name, including any aliases;
  - (ii) Unique Identification Number (such as an Identity card number, passport number, etc.);
  - (iv) Date of birth;
  - (iv) Nationality;
  - (v) Legal domicile;
  - (vi) Current residential address; (other than a post office box address);
  - (vii) Contact details such as personal, office or work telephone numbers.
- (b) If a customer is a legal person or legal arrangement, we shall obtain at least the following information:
  - (i) The full name and any trading name;
  - (ii) Unique identification Number (i.e., Tax identification number or equivalent where this exists, incorporation number or business registration number);
  - (iii) Registered or business address, and if different, its principal place of business;
  - (iv) Date of establishment, incorporation or registration;
  - (iv) Place of incorporation or registration.
- (c) Further, in cases where the customer is a legal person or legal arrangement, we shall also identify the legal form, constitution and powers that regulate and bind the legal person or legal arrangement. In addition to this, we shall also identify and screen the related parties or connected parties of such customer and should remain apprised of any changes to connected parties. For identification of the connected parties, obtain at least the following information of each related or connected party:
  - (i) full name, including any aliases; and
  - (ii) Unique Identification Number (such as an Identity card number, passport number, etc.).

- (d) In accordance with the IFSCA (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022 (AML CFT Guidelines), broker dealers, depository participants and custodians in the IFSC are required to conduct KYC and CDD including identification of beneficial owners.

All broker dealers, depository participants and custodians, after conducting KYC and CDD, shall maintain a list of all clients that meet any of the following conditions:

- i. The Client is a citizen of a country sharing land border with India;*
- ii. The Client is incorporated in a country sharing land border with India; or*
- iii. Any beneficial owner of the client is situated in or is a citizen of a country sharing land border with India.*

This list shall be updated at the time of each on-boarding of a new client, in addition to its periodic updation in accordance with the applicable periodicity under the AML CFT Guidelines.

The list prepared by the broker dealers shall be shared with the respective Stock Exchanges in the IFSC for the purpose of monitoring and conducting market surveillance. Any updation by a broker dealer in the list shall be immediately informed to the respective stock exchanges, within one working day of such updation.

The list prepared by the depository participants shall be shared with the Depository, and the depository in turn shall share the same with the recognised stock exchanges in IFSC. Any updation by a depository participant in the list shall be immediately informed to the depository, within one working day of such updation.

### **Declaration by Clients**

**a) Clients from countries sharing land border with India**

Broker dealers, depository participants and custodians shall take a signed declaration from all their clients falling above (“Identified Clients”) that they shall not hold equity shares of a public Indian company listed or proposed to be listed on a stock exchange in IFSC, without prior approval of the Central Government.

This declaration shall be taken at the time of initial on-boarding and also at the time of periodic updation of client due diligence.

**b) Clients from other countries**

Broker dealers, depository participants and custodians shall take a signed declaration from all other clients stating that neither the client nor any of its beneficial owners, as defined under the PML Rules read with AML CFT Guidelines, is situated in or is a citizen of a country sharing land border with India. This declaration shall be taken at the time of initial on-boarding and also at the time of periodic updation of client due diligence.

**3.4.3. Verification of Identity of Customer**

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

**In case of Natural Persons –**

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

**In case of Legal persons or Legal Arrangements-**

- (i) **Name, legal form, proof of existence and constitution:-** the verification for the same can be obtained from certificate of incorporation, certificate of good standing, partnership deed/ agreement, trust deed, constitutional document, certificate of registration or any other document from a reliable independent source; and
- (ii) **Powers that regulate and bind the legal person or legal arrangement:-** This can be ascertained from the constitutional documents, as well as the names of the relevant persons having a Senior Management position in the legal person or legal arrangement and board resolution or similar document authorising the opening of an account and appointment of its authorised signatories.

**3.4.4. Identification and Verification of Identity of Natural Person appointed to act on behalf of Customer**

- (a) Where a customer is a natural person or legal person, and appoints one or more natural persons to act on its behalf for establishing business relations with us,

we shall identify each natural person who acts or is appointed to act on behalf of such natural or legal person by obtaining information as specified in Clause 3.4.2 above.

- (b) Further, we shall verify the identity of each such natural persons using reliable, independent source data, documents or information. Furthermore, we shall verify the authorisation of each natural person appointed to act on behalf of the customer by obtaining at least the following:
  - (i) The appropriate documentary evidence authorising the appointment of such natural person by the customer to act on his or its behalf which may include power of attorney, resolution passed by Governing Body or authorisation granted to transact on its behalf.
  - (ii) Where there is a long list of natural persons appointed to act on behalf of the customer (e.g. a list comprising more than 10 authorized signatories), verify those natural persons who will deal directly with the Regulated Entity.

### **3.4.5. Identification and Verification of Identity of Beneficial Owners**

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

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

#### **(a) Customers that are legal persons**

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

#### **(b) Customers that are legal arrangements**

- (i) Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen per cent. or more interest in the trust and any

other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

- (ii) In all other types of legal arrangements, identify persons in equivalent or similar positions.

#### 3.4.6. Parameters to Identify and Verify the Identity of Beneficial Owners: -

- (a) Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.

***Explanation-*** For the purpose of this sub-clause-

“Controlling ownership interest” means ownership of or entitlement to **ten per cent (10%)** or more of the shares or capital or profits of the company; “Control” shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;

*We shall also collect the names of the relevant persons holding senior management position; and the registered office and the principal place of its business, if it is different.*

- (b) Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/ have ownership of/ entitlement to **ten per cent (10%)** or more of capital or profits of the partnership;

*We shall collect the names of all the partners and address of the registered office, and the principal place of its business, if it is different.*

- (c) Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/ have ownership of or entitlement to **ten per cent (10%)** or more of the property or capital or profits of the unincorporated association or body of individuals.

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

- (d) Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with

**ten per cent (10%)** or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

*We shall also collect the names of the beneficiaries, trustees, settlor and authors of the trust and the address of the registered office of the trust; and obtain list of trustees and documents as are required for individuals for those discharging role as trustee and authorised to transact on behalf of the trust.*

- 3.4.7.** As per Rules, unless we have doubts about the veracity of the CDD information, or suspects that customer may be connected with ML/TF, it shall not be required to identify and verify the identity of any shareholder or beneficial owner of a customer in the following -

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

- 3.4.8.** As per the Rules, in cases where a customer is subscribing or dealing with depository receipts or equity shares issued or listed in jurisdictions notified by the Central Government, of a company incorporated in India, and it is acting on behalf of a beneficial owner who is resident of such jurisdiction, the determination, identification and verification of such beneficial owner, shall be as per the norms of such jurisdiction.

**3.4.9. Information on the Purpose and Intended Nature of Business Relations**

- (a) We shall, while establishing business relationship, understand and as appropriate, obtain information from the customer as to the purpose and intended nature of business relations.
- (b) The measures taken by us to understand the purpose and intended nature of business relations should be commensurate with the risk profile and complexity of the customer's business.

**3.5. Accounts of Politically Exposed Persons**

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

- (a) We shall implement appropriate internal risk management systems, policies and procedures to determine if a customer or any natural person appointed to act on behalf of the customer, or any beneficial owner of the customer is a politically exposed person (PEP).
- (b) We shall, in addition to undertaking CDD measures, undertake at least the following additional measures where a customer or any beneficial owner of the customer, or a Beneficial Owner of a beneficiary is determined to be a PEP:
  - (i) Collect by appropriate and reasonable means, adequate information including information about the source of wealth and income of family members, any beneficial owner and close relatives;
  - (ii) Verify the identity before accepting the PEP as a customer;
  - (iii) Obtain approval from its Senior Management before opening an account of a PEP or making any payout under the life insurance or other similar policy to the PEP;
  - (iv) In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, obtain the Senior Management's approval to continue the business relationship;
  - (v) Increase the degree and nature of ongoing monitoring of the business relationship, to determine whether the customer's transactions or activities appear unusual or suspicious.
  - (vi) Carry out the additional Customer Due Diligence for circumstances specified in sub-clauses (i) to (v) above, before making any payout.
- (c) we may adopt a risk-based approach in determining whether to perform enhanced CDD measures or the extent of enhanced CDD measures to be performed for:-
  - (i) PEP, their family members and close associates;
  - (ii) International Organisation PEP, their family members, and close associates; or
  - (iii) PEP who have stepped down from their prominent public functions, taking into consideration the level of influence such persons may continue to exercise after stepping down, their family members and close associates, except in cases where their business relations or transactions with us present a high risk for ML/TF.

**3.6. Enhanced Due Diligence**

- (a) Where the risks of ML/TF are high, we shall conduct enhanced CDD measures, consistent with the risks identified. The enhanced CDD measures are as follows:
- - (i) Obtaining additional information on the customer (e.g., occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.
  - (ii) Obtaining information and taking additional steps to examine the ownership and financial position, including source of wealth and source of funds of the customer or, if applicable, of the Beneficial Owner.
  - (iii) Obtaining information and taking additional steps to record the purpose behind conducting the specified transaction and the intended nature of the relationship between the transaction parties.
  - (iv) Obtaining the approval of Senior Management to commence or continue the business relationship.
  - (v) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination; and,
  - (vi) Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.
- (b) Where applicable, it is required that first payment made by a customer in order to open an account with us shall be carried out through a bank account in the customer's name with:
- (i) a Bank;
  - (ii) a regulated financial institution whose entire operations are subject to regulation and supervision, including AML/CFT regulation and supervision, in a jurisdiction where its regulations on AML/CFT are equivalent to the standards set out in the FATF recommendations; or
  - (iii) a subsidiary of a regulated financial institution referred to in (ii), if the law that applies to the Parent entity ensures that the subsidiary also observes the same AML/CFT standards as its Parent entity.

**3.7. Simplified Customer Due Diligence**

- (a) Where the risks of ML/TF are low, we may conduct simplified CDD measures, which should be commensurate with the low risk factors. Examples of possible measures are:
  - (i) Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship as specified under Clause 5.3.
  - (ii) Reducing the frequency of customer identification updates.
  - (iii) Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.
  - (iv) Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship but inferring the purpose and nature from the type of transactions or business relationship established.
- (b) Simplified CDD (SCDD) measures shall not be conducted where there is a suspicion of ML/TF.

**3.8. Ongoing customer due diligence**

While undertaking the ongoing customer due diligence, as required under Clause 3.4.1.(d), the following requirements shall be complied: -

- (i) Monitor business relations with the customer on an ongoing basis.
- (ii) We during the course of business relations with a customer, shall observe the conduct of the customer's account and scrutinize transactions undertaken throughout the course of business relations, to ensure that the transactions are consistent with our knowledge of the customer, its business and risk profile and where appropriate, may seek the source of wealth and source of funds.
- (iii) We shall pay particular attention to any complex, unusually large or unusual patterns of transactions undertaken throughout the course of business relations, that have no apparent or visible economic or legitimate purpose.
- (iv) We shall make further enquiries into the background and purpose of the transaction specified in sub-clause (iii) above and document its findings so that this information is made available to the relevant authorities, should the need arise.

- (v) We shall periodically review each customer to ensure that the risk rating assigned is commensurate with the ML/TF risks posed by the customer.
- (vi) Where there are indications that the risks associated with an existing business relation with the customer may have increased, we shall request additional information and conduct a review of the customer's risk profile in order to determine if additional measures are necessary.
- (vii) We shall ensure that the Customer Due Diligence data, documents and information obtained in respect of customers, natural persons appointed to act on behalf of the customers, related parties of the customers and beneficial owners of the customers, are relevant and kept up-to-date by undertaking the review of adequacy of the existing Customer Due Diligence data, documents and information, particularly for customers with high-risk rating.

**3.9. Ongoing sanctions screening**

We shall review its customers, their business and transactions against United Nations Security Council sanctions lists and also against any other relevant sanctions list when complying with Clause 3.4.1 (d).

**3.10. Failure of Regulated Entity to conduct or complete customer due diligence**

- (a) In cases where we are unable to conduct or complete the requisite Customer Due Diligence for a customer in accordance with Clause 3.4.1, it, to the extent relevant, shall:-
  - (i) not open an account or otherwise provide a service;
  - (ii) not carry out a transaction with or for the customer;
  - (iii) not otherwise establish a business relationship;
  - (iv) terminate or suspend any existing business relationship with the customer;
  - (iv) return any monies or assets received from the customer; and,
  - (v) consider whether the failure to conduct or complete Customer Due Diligence necessitates the filing of a Suspicious Transaction Report (STR).
- (b) We are not bound to comply with sub-clauses (a) (i) to (v) above, if it amounts to “tipping off” of the customer, or FIU-IND directs the Regulated Entity to act otherwise.

**3.11. Periodic Updation**

The periodicity of updation from the date of opening of the account/ last CDD updation for different categories of customers is as follows: -

- (i) Once in a two years for high-risk customers- ;
- (ii) Once in a five years for medium risk customer; and,
- (iii) Once in an eight years- for low-risk customers.

**(a) Individual Customers:****(i) No change in CDD information:**

In case of no change in the CDD information, a self-declaration from the customer in this regard may be obtained through mobile number registered with us or through e-mail.

**(ii) Change in address:**

- (aa) In case of a change only in the address details of the customer, a self-declaration of the new address may be obtained from the customer through customer's email-id registered with us. The declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.
- (bb) Further, we shall obtain a copy of OVD or the equivalent e-documents thereof for the purpose of proof of address declared by the customer at the time of periodic updation.

**(b) Customers other than Natural Persons:****(i) No change in CDD information:**

In case of no change in the CDD information of a customer, which is a non natural person, a self declaration through email id registered with us, a letter duly signed by authorized official and requisite resolutions in this regard shall be obtained from the customer. Further, we shall ensure that Beneficial Ownership (BO) information available with them is accurate and upto-date.

**(ii) Change in CDD information:**

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

**(c) Additional measures:**

In addition to the above, we shall ensure that:

- (i) The KYC documents of the customer as per the current CDD standards are available with it. This is applicable even if there is no change in customer information but the documents available with us are not as per the current CDD standards. Further, in case the validity of the CDD documents available with us has expired at the time of periodic updation of CDD, we shall undertake fresh CDD process equivalent to that applicable for on boarding a new customer.
- (ii) In case of Indian National, the customer's PAN details, if available with us, is verified from the database of the issuing authority at the time of periodic updation of CDD.
- (iii) Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, we shall ensure that the information/documents obtained from the customers at the time of periodic updation of

CDD are promptly updated in its records/ database and an intimation, mentioning the date of updation of CDD details, is provided to the customer.

- (iv) In order to ensure customer convenience, we may consider making available the facility of periodic updation of CDD at any of our branch.
- (v) We shall ensure that internal KYC policy and processes on updation/ periodic updation of CDD are transparent and adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements.

**CHAPTER-4****INTERNAL POLICIES, COMPLIANCE, AUDIT AND TRAINING****4.1. Internal Policies**

Develop and implement adequate internal policies, procedures, and controls, taking into consideration its ML/ TF risks and the size of business, to help prevent ML/ TF, and communicate these to its employees.

**4.2. Compliance**

- (a) Develop appropriate compliance management, including appointing or designating a Principal Officer at the management level and shall also develop compliance framework.
- (b) Ensure that the Principal Officer, as well as any other persons appointed to assist him, is suitably qualified and, has adequate resources and timely access to all customer records and other relevant information which he may require to discharge his functions.
- (c) Ensure that the Principal Officer has the necessary seniority and authority within the Regulated Entity to effectively perform his responsibilities.
- (d) The responsibilities of the Principal Officer shall include:
  - (i) carrying out, or overseeing the carrying out of, ongoing monitoring of business relations for compliance with these Guidelines;
  - (ii) promoting compliance of these Guidelines and taking overall charge of all AML/CFT matters within the organisation;
  - (iii) informing employees, officers and representatives promptly of regulatory changes;
  - (iv) ensuring a speedy and appropriate reaction to any matter in which ML/TF is suspected;
  - (iv) reporting or overseeing the reporting of suspicious transactions;
  - (v) advising and training employees, officers and representatives on developing and implementing internal policies, procedures and controls on AML/CFT;

- (vi) reporting to Senior Management on the outcome of reviews of the Regulated Entity's compliance with these Guidelines & risk assessment procedures; and
  - (vii) reporting regularly on key AML/CFT risk management and control issues, and any necessary remedial actions, arising from audit, inspection & compliance reviews to the Regulated Entity's Senior Management.
- (e) The business interests should not interfere with the effective discharge of the above-mentioned responsibilities of the Principal Officer and potential conflicts of interest should be avoided.
- (f) To enable unbiased judgments and facilitate impartial advice to management, the Principal Officer should be distinct from the internal audit and business line functions. Where any conflict between business lines and the responsibilities of the Principal Officer arises, procedures should be in place to ensure that AML/CFT concerns are objectively considered and addressed at the appropriate level of the Regulated Entity's management.

#### **4.3. Audit**

- (a) A Regulated Entity shall maintain an audit function that is adequately resourced and independent, that is able to regularly assess the effectiveness of the Regulated Entity's internal policies, procedures and controls, in compliance with regulatory requirements and these Guidelines.
- (b) A Regulated Entity's AML/CFT framework should be subjected to periodic audits. Such audits should be performed not just on individual business functions but also on a Regulated Entity-wide basis. Auditors should assess the effectiveness of measures taken to prevent ML/TF. This would inter-alia include —
- (i) Determining the adequacy of the Regulated Entity's AML/CFT policies, procedures and controls, ML/TF risk assessment framework and application of risk-based approach;
  - (ii) Reviewing the content and frequency of AML/CFT training programmes, and the extent of employee's, officer's and representative's compliance with established AML/CFT policies and procedures; and
  - (iii) Assessing whether instances of non-compliance are reported to Senior Management on a timely basis. The frequency and extent of the audit should be commensurate with the ML/TF risks presented and the size and complexity of the Regulated Entity's business.

**4.4. Training and awareness**

We shall: -

- (a) provide AML/CFT training to all relevant employees, periodically;
- (b) ensure that its AML/ CFT training enables its employees to:
  - (i) comprehend the applicable laws relating to ML/TF, including the Act and Rules;
  - (ii) understand its policies, procedures, systems and controls related to AML/CFT and any amendments/modifications thereto;
  - (i) recognise and deal with transactions and other activities which may be related to ML/TF;
  - (iv) comprehend the kind of activity that may constitute suspicious activity, which warrants prompt notification to the Principal Officer;
  - (v) have knowledge of the prevailing techniques, methods and trends in ML/TF, relevant to the business of company;
  - (vi) understand their roles and responsibilities in combating ML/ TF, including the identity and duties of Principal Officer;
  - (vii) understand the relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions described in Chapter VI.
- (c) ensure that its AML/ CFT training:
  - (i) is relevant and tailored to the company's activities, including its products, services, customers, distribution channels, business partners, level and nature of its transactions; and
  - (ii) identifies and indicates the different levels of ML/ TF risk and vulnerabilities associated with the matters in sub-clause (c)(i) above.

**CHAPTER-5****RECORD KEEPING****5.1.** Maintain the following records:

- (a) a copy of all documents and information obtained in undertaking initial and ongoing Customer Due Diligence;
- (b) records of customer business relationships (both original and certified copies), which include: -
  - (i) correspondence of business and other information relating to a customer's account;
  - (ii) adequate records of transactions to enable standalone transactions to be reconstructed; and
  - (iii) internal findings and analysis relating to a business transaction or other transactions, where the transaction or business may be unusual or suspicious, whether or not it results in a Suspicious Transactions Report;
- (c) notifications made under Clause 10.1. (b);
- (d) Suspicious Transactions Reports and any relevant supporting documents and information, including internal findings and analysis;
- (e) any relevant communications, if made with the FIU;
- (f) the documents referred to in Clause 6.4; and
- (g) any other matter that may be expressly required to record and maintain, under these Guidelines.

**5.2.** Preserve all necessary records, for at least six years or for such period as prescribed under the applicable laws, from the date on which business relationship has ended or transaction is completed.**5.3.** Provide to the Authority or any law enforcement agency immediately on request, a copy of a records maintained by it under these Guidelines.**5.4. Risk Assessment Documents**

Keep and maintain all risk assessment documents and provide to the Authority immediately on request, all relevant documents and information, including: -

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

**5.5.** Where the records referred to in Clause 6.1 are kept by us outside the IFSC, we shall:

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

**5.6.** We shall:

- (a) verify if there are secrecy or data protection laws that would restrict access without delay to the records referred to in Clause 6.1, by us, the Authority or the law enforcement agencies of India; and
- (b) where such law exists, obtain without delay, the certified copies of the relevant records and keep such copies in a jurisdiction which allows access by those persons referred in Clause (a) above.

**5.7.** We shall be able to convey that we have complied with the training requirements through appropriate measures, including the maintenance of relevant training records.

## **CHAPTER-6**

### **PROCESS OF IDENTIFICATION OF SUSPICIOUS TRANSACTIONS**

#### **6.1. Internal reporting requirements**

- (a) Establish and maintain policies, procedures, systems and controls in order to monitor and detect suspicious transactions with respect to potential ML/ TF.
- (b) Put in place such policies, procedures, systems and controls which ensure that whenever any of its employee, acting in the ordinary course of his employment, either:
  - (i) knows;
  - (ii) suspects; or
  - (iii) has reasonable grounds for knowing or suspecting;

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

#### **6.2. Indications of Suspicious Transactions**

We can identify suspicious transactions by following these four steps:

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

##### **(a) Detect suspicious indicators**

The first step in identifying a suspicious transaction is to detect indicators that a transaction(s) may involve funds that are derived from an illegal activity or that the transaction(s) is an attempt to disguise funds derived from illegal activity or lacks a business or apparent lawful purpose.

##### **(b) Ask Customer Questions**

- (i) If one or more suspicious indicators are detected, the Regulated Entity and its employees may ask the customer relevant and appropriate questions to determine whether there is a reasonable explanation for that observed indicator.

- (ii) The Regulated Entity shall ensure that when asking such questions, they do not “tip-off” the customer. Instead, questions could be asked using a service approach.

(c) **Review Customer’s Records**

The next step is to determine whether the suspicious indicators identified earlier is justifiable given what is known about the customer. To achieve this, we shall review its customer’s records and consider all information that is already known to it about the customer. This may include:

- (i) the customer’s usual occupation, business or principal activity;
- (ii) the customer’s transaction history;
- (iii) the customer’s risk profile;
- (iv) the customer’s income level;
- (v) the customers source of income as stated during account opening or initial engagement;
- (vi) reasons for the transactions as provided by the customer;
- (vii) the “relationship” of the customer with the sender or beneficiary of funds;
- (viii) the frequency of transactions;
- (ix) the size and complexity of the transaction;
- (x) the identity or location of any other person(s) involved in the transaction;
- (xi) the usual or typical financial, business or operational practices or behavior of customers in the similar occupation or business category; and
- (xii) the availability of identification documents and other documentation. After reviewing as aforesaid if the Regulated Entity finds that the customer’s profile has changed, it shall update the customer’s profile.

(d) **Evaluate Information Collected**

- (a) We shall evaluate the:
  - (i) suspicious indicators,

- (ii) information solicited from the customer through questions asked, and
  - (iii) known information about the customer to determine if there are reasonable grounds to suspect that the transaction(s) is related to the commission of a ML/ TF or any other serious offence.
- (b) If we conclude that there are reasonable grounds to suspect that the transaction(s) or attempted transaction(s) is linked to a ML/ TF or any other serious offence, it should report this suspicion to the FIU-IND by completing and submitting a STR.

### **REPORTING OF SUSPICIOUS TRANSACTIONS**

#### **6.3. Reporting Requirements to Financial Intelligence Unit – India**

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

We shall carefully go through all the reporting requirements and formats as suggested by FIU-IND. We shall adhere to the following:

- a) The Suspicious Transaction Report (STR) shall be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion.
- b) The Principal Officer will be responsible for timely submission of STR to FIU-IND;
- c) Utmost confidentiality shall be maintained in filing of STR to FIU-IND.
- d) No nil reporting needs to be made to FIU-IND in case there are no suspicious transactions to be reported.
- e) We shall not put any restrictions on operations in the accounts where an STR has been made. Our directors, officers and employees (permanent and temporary) shall be prohibited from disclosing (“tipping off”) the fact that a STR or related information is being reported or provided to the FIU-IND. This prohibition on tipping off extends not only to the filing of the STR and/ or related information but

even before, during and after the submission of an STR. Thus, it shall be ensured that there is no tipping off to the client at any level.

- f) It is clarified that the registered intermediaries, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, shall file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.

#### **6.4. Confidentiality of Suspicious Transaction Report (STR)**

- (a) Any employee shall not disclose to any person (including the customer):
  - (i) that it has reported or will be reporting a suspicious transaction to the FIU-IND;
  - (ii) that it has formed a suspicion on a particular customer's transaction; or
  - (iii) any other information which may cause the person to conclude that a suspicion has been formed or that a report has been or may be made to the FIU-IND.
- (b) Disclosure of information on suspicious transactions is only allowed under the following circumstances:
  - (i) disclosure to an officer/ employee for any purpose connected to the performance of that person's duties;
  - (ii) disclosure to a lawyer for the purpose of obtaining legal advice on the matter;
  - (iii) disclosure to a supervisory authority (to enable it to carry out its supervisory role); or
  - (iv) disclosure in compliance with the court order.
- (c) Company and its employees are protected from any civil, criminal or disciplinary action taken against them for reporting a suspicious transaction in good faith.

**6.5. Additional measures**

- (a) Lawyers, notaries, accountants, and entities offering such services shall report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the following activities:-
  - (i) buying and selling of real estate;
  - (ii) managing of client money, securities or other assets;
  - (iii) management of bank, savings or securities accounts;
  - (iv) organization of contributions for the creation, operation or management of companies;
  - (v) creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

**6.6. Appointment of Designated Director**

“Designated Director” means a person designated by the Regulated Entity to ensure overall compliance with the obligations imposed under Chapter IV of the Act, the Rules and these Guidelines. Names, designation and addresses (including e-mail addresses) of ‘Designated Director’ including any changes therein shall also be intimated to the Office of the Director-FIU.

**6.7. Appointment of Principal Officer**

To ensure that company properly discharge their legal obligations to report suspicious transactions to the authorities, the Principal Officer would act as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in the Identification and assessment of potentially suspicious transactions and shall have access to and be able to report to senior management at the next reporting level or the Board of Directors. Names, designation and addresses (including e-mail addresses) of ‘Principal Officer’ including any changes therein shall also be intimated to the Office of the Director-FIU.

**CHAPTER- 7****COMPLIANCE OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS AND DOMESTIC LAWS****7.1. Requirements/ obligations under International Agreements Communications from International Agencies –**

- (a) ensure that in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, we do not have any account in the name of individuals/ entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:

- (i) The “ISIL (Da’esh) & Al-Qaida Sanctions List”, which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al- Qaida Sanctions List is available at:

<https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl>

- (ii) The “1988 Sanctions List”, consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at:

<https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl>

- (b) Details of accounts resembling any of the individuals/ entities mentioned in the above lists, shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA Order bearing file no.14014/01/2019/CFT dated February 2, 2021, issued by the CTCR Division of the Ministry of Home Affairs, Government of India, which is available at [https://www.mha.gov.in/sites/default/files/ProcedureImplementationSection51A\\_30032021.pdf](https://www.mha.gov.in/sites/default/files/ProcedureImplementationSection51A_30032021.pdf)
- (c) In addition to the above, other UNSC Resolutions circulated by the IFSCA in respect of any other jurisdictions/ entities from time to time, shall also be taken note of for necessary compliances.

**7.2. Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967**

The procedure laid down in the UAPA Order bearing file no.14014/01/2019/CFT dated February 2, 2021, issued by the CTCR Division of the Ministry of Home Affairs, Government of India, shall be strictly followed and compliance with the Order shall be

ensured. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

**7.3. Jurisdictions that do not or insufficiently apply the FATF Recommendations**

- (a) FATF Statements circulated from time to time, and publicly available information for identifying countries which do not or insufficiently apply the FATF Recommendations, shall be considered. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account.
- (b) Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or emanating in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in the FATF statements.

**Explanation:** The process referred to in (a) and (b) above, do not preclude Regulated Entities from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

- (c) The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations as aforesaid shall be examined, and written findings, together with all documents, shall be retained and be made available to the Authority and other relevant authorities, on request.

**7.4. Secrecy Obligations and Sharing of Information:**

- (a) We shall maintain secrecy regarding the customer information that arises out of the contractual relationship between us and the customer.
- (b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged without the express consent of the customer.
- (c) While considering the requests for data/ information from Government and other agencies, we shall satisfy itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy.
- (d) The exceptions to the above obligations shall be as under:
  - (i) Where disclosure is under compulsion of law;
  - (ii) Where there is a duty to the public to disclose;
  - (iii) Where the interest of Regulated Entity requires disclosure; and
  - (iv) Where the disclosure is made with the express or implied consent of the customer.

**7.5. Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)**

Under FATCA and CRS, we shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether it is a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements:

- (a) Register on the related e-filing portal of Income Tax Department as Reporting Financial Institutions at the link: <https://incometaxindiaefiling.gov.in/> post login > My Account --> Register as Reporting Financial Institution;
- (b) Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.

**Explanation:** We shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at <https://fedai.org.in/> for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H.

- (c) Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.
- (d) Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.
- (e) Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.
- (f) Ensure compliance with updated instructions/ rules/ guidance notes/ Press Releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time and available on the web site <http://www.incometaxindia.gov.in/Pages/default.aspx>. We shall also take note of the following:
  - (i) updated Guidance Note on FATCA and CRS; and
  - (ii) a press release on 'Closure of Financial Accounts' under Rule 114H.

**7.6. Sharing of KYC information pertaining to Indian Resident (Natural and Legal Entities) with Central KYC Records Registry (CKYCR):**

- (a) We shall capture customer's KYC records and upload on CKYCR within 10 days of commencement of an account-based relationship with the customer in the form and manner as prescribed under Central KYC Registry Operating Guidelines 2016, released by Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI) and shall ensure that:
  - (i) the KYC records to be uploaded are as per KYC Template released by CERSAI.
  - (ii) Once KYC Identifier is generated by CKYCR, the same is communicated to the Customer.
  - (iii) It has performed the last KYC verification or has sent updated information in respect of a Customer to CKYCR.
- (b) Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to us with an explicit consent to download records from CKYCR, we shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –
  - (i) there is a change in the information of the customer as existing in the records of CKYCR;
  - (ii) the current address of the customer is required to be verified; and,
  - (iii) the Regulated Entity considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

**CHAPTER-8****GROUPS, BRANCHES AND SUBSIDIARIES****8.1. Obligation to develop and ensure implementation of KYC/AML-CFT standards**

- (a) develop a group policy on AML/ CFT to meet the requirements of these Guidelines and extend the same to all of its branches and majority owned subsidiaries. The group policies should include:
  - (i) the development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees;
  - (ii) an ongoing employee training programme; and
  - (iii) an independent audit function to test the system.
- (b) communicate the group policy to all its branches and majority owned subsidiaries and ensure its implementation.
- (c) Where the KYC/AML-CFT standards in another jurisdiction differ from those specified by the Authority, we shall require its branch or majority owned subsidiary in that jurisdiction to apply the higher of the two standards, to the extent permitted by the law of that jurisdiction.
- (d) Where the law of another jurisdiction does not permit the implementation of KYC/ AML-CFT standards that are equivalent to or higher than those that apply to us incorporated in an IFSC, we shall: -
  - (i) inform the Authority in writing; and
  - (ii) apply appropriate additional measures to prevent the ML/ TF risks posed by the relevant branch or subsidiary.
- (e) Where we have a branch or subsidiary in a country or jurisdiction:
  - (i) For which the FATF has called for countermeasures; or
  - (ii) It is known to have inadequate AML/CFT measures, as identified by us for our self or notified by the Authority or other foreign regulatory authorities to us;

We shall ensure that our group policy on KYC-AML-CFT standards is strictly observed by the management of that branch or subsidiary.

**8.2. Group Policy**

We as a part of a Financial Group must ensure that it:

- (a) has developed and implemented its group policies and procedures for the sharing of information between Financial Group entities, including the sharing of information related to CDD and for ML/TF risk management;
- (b) has put in place adequate safeguards to protect the confidentiality and use of any information that is exchanged between Financial Group entities;
- (c) remains aware of the ML/TF risks of the Financial Group as a whole, of its exposure to the Financial Group and takes active steps to mitigate such risks;
- (d) contributes to a Group-wide risk assessment to identify and assess ML/TF risks for the Financial Group;
- (e) provides its Group-wide compliance, audit and AML/CFT functions of customer, account, and transaction information from its branches and subsidiaries, when necessary for the purposes of ML/TF risk management.