**KYC Standards and AML Policy (Generalized)**

This policy outlines the Know Your Customer (KYC) Standards and Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT) framework for a **Regulated Entity**. It is framed in line with the **Regulatory Authority** Master Direction on Know Your Customer (KYC) and other relevant acts and rules, as amended from time to time.

The policy aims to prevent financial institutions from being used as channels for Money Laundering (ML) and Terrorist Financing (TF) and to ensure the integrity and stability of the financial system.

**1. Title and Commencement**

This policy is framed in line with the **Regulatory Authority** Master Direction - Know Your Customer (KYC) Direction, 2016, updated as on November 06, 2024.

**2. Applicability of AML KYC Policy**

The provisions of these Directions will apply to the branches, subsidiaries, and majority-owned joint ventures located abroad, to the extent local laws permit, of the **Regulated Entity**.

* Each foreign office of the **Regulated Entity** is required to put in place an Anti-Money Laundering Policy (duly approved) which shall also contain the KYC guidelines and Suspicious Activity Reporting (SAR) procedures as may be required by the rules and regulations of the host country.
* Where applicable laws and regulations prohibit implementation of these guidelines, the same will be brought to the notice of the **Regulatory Authority**.
* The **Regulatory Authority** may advise further necessary action by the **Regulated Entity** including application of additional measures to be taken to manage the ML/TF risks.
* In case there is a variance in KYC/AML standards prescribed by the **Regulatory Authority** and the host country regulators, branches/subsidiaries of **Regulated Entities** are required to adopt the more stringent regulation of the two.
* This rule shall not apply to 'small accounts' as referred to in Serial no:18 of Customer Due Diligence (CDD) Procedure of this policy.

**3. Definitions**

Terms used in this policy bear meanings assigned in terms of the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, unless the context otherwise requires.

Key definitions include:

* **Authentication (Aadhaar):** The process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
* **Beneficial Owner (BO):**
  + **Company:** The natural person(s) who, alone or together, or through one or more juridical persons, has/have a controlling ownership interest (more than 10% of shares, capital, or profits) or who exercise control through other means (right to appoint majority directors, control management or policy decisions).
  + **Partnership Firm:** The natural person(s) who, alone or together, or through one or more juridical persons, has/have ownership of/entitlement to more than 10% of capital or profits, or who exercises control through other means.
  + **Unincorporated Association or Body of Individuals:** The natural person(s) who, alone or together, or through one or more juridical persons, has/have ownership of/entitlement to more than 15% of the property or capital or profits. If no natural person is identified, the beneficial owner is the relevant natural person who holds the position of senior managing official.
  + **Trust:** Includes identification of the author of the trust, the trustee, beneficiaries with 10% or more interest, and any other natural person exercising ultimate effective control.
* **Certified Copy:** Obtaining a certified copy by the **Regulated Entity** means comparing the copy of the proof of possession of Aadhaar number (where offline verification cannot be carried out) or officially valid document with the original and recording the same on the copy by the authorized officer. For Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), certified copies can be obtained from authorized officials of overseas branches of Scheduled Commercial Banks registered in India, branches of overseas banks with whom Indian banks have relationships, Notary Public abroad, Court Magistrate, Judge, or Indian Embassy/Consulate General in the country where the non-resident customer resides.
* **Central KYC Records Registry (CKYCR):** An entity defined under Rule 2(1) of the Rules, to receive, store, safeguard, and retrieve the KYC records in digital form of a customer.
* **Designated Director:** A person designated by the board to ensure overall compliance with obligations under Chapter IV of the PML Act and the Rules, including the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the Reporting entity is a company.
* **Digital KYC:** Capturing live photo of the customer and an officially valid document (OVD) or proof of possession of Aadhaar (where offline verification cannot be carried out), along with the latitude and longitude of the location, by an authorized officer of the **Regulated Entity**.
* **Equivalent e-document:** An electronic equivalent of a document, issued by the issuing authority with its valid digital signature, including documents issued to the digital locker account.
* **Know Your Client (KYC) Identifier:** The unique number or code assigned to a customer by the Central KYC Records Registry.
* **Non-profit organizations (NPO):** Any entity or organization constituted for religious or charitable purposes, registered as a trust or a society, or a company registered under Section 8 of the Companies Act, 2013.
* **Officially Valid Documents (OVD) [for individuals]:** Passport, Driving License, Proof of possession of Aadhaar number, Voter's Identity Card, Job card issued by NREGA, letter issued by the National Population Register, or any document notified by the **Regulatory Authority**/Government.
  + **Proof of Address (if OVD doesn't have updated address):** Utility bill (not more than two months old), property or Municipal tax receipt, pension or family pension payment orders (PPOs) (if they contain address), letter of allotment of accommodation from employer (government, PSU, SCBs, FIs, listed companies) and leave and license agreements. The customer must submit Aadhaar or OVD updated with current address within three months. For foreign nationals, documents issued by government departments of foreign jurisdictions and letters from Foreign Embassy or Mission in India are accepted as proof of address.
* **Offline verification:** As defined in the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
* **Person:** Includes an individual, Hindu undivided family, company, firm, association of persons or body of individuals, artificial juridical person, and any agency, office or branch owned or controlled by any of the above.
* **Principal Officer:** An officer at the management level nominated by the **Regulated Entity**, responsible for furnishing information as per rule 8 of the Rules.
* **Suspicious transaction:** Any transaction, including an attempted transaction, that gives rise to a reasonable suspicion of involving proceeds of an offence, appears to be of unusual complexity, lacks economic rationale or bona-fide purpose, or involves financing of terrorism activities.
* **Small Account:** A savings account opened in terms of sub-rule (5) of rule 9 of the PML Rules, 2005.
* **Transaction:** Includes opening of an account, deposit, withdrawal, exchange or transfer of funds, use of a safety deposit box, entering into fiduciary relationship, any payment for contractual or legal obligation, or establishing a legal person or arrangement.
* **Video based Customer Identification Process (V-CIP):** A method of customer identification by an official of the **Regulated Entity**, by undertaking seamless, secure, real-time, consent-based audio-visual interaction with the customer to obtain identification information and ascertain veracity of information through independent verification and maintaining audit trail. This is treated on par with face-to-face CIP.
* **Group:** The term "group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act, 1961.
* **Common Reporting Standards (CRS):** Reporting standards for implementation of multilateral agreement to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.
* **Customer:** A person engaged in a financial transaction or activity with a **Regulated Entity** and includes a person on whose behalf the transaction is being conducted.
* **Walk-in Customer:** A person who does not have an account-based relationship with the **Regulated Entity**, but undertakes transactions.
* **Customer Due Diligence (CDD):** Identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification. This includes identification and verification, understanding business nature, ownership and control, and identifying and verifying beneficial owners.
* **Customer identification:** Undertaking the process of CDD.
* **FATCA:** Foreign Account Tax Compliance Act of the USA, requiring foreign financial institutions to report about financial accounts held by U.S. taxpayers.
* **IGA:** Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA.
* **KYC Templates:** Templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
* **Non-face-to-face customers:** Customers who open accounts without visiting the branches/offices of the **Regulated Entities** or meeting their officials.
* **On-going Due Diligence:** Regular monitoring of transactions in accounts to ensure consistency with the **Regulated Entity's** knowledge about the customers, their business and risk profile, and source of funds/wealth.
* **Periodic Updation:** Steps taken to ensure that documents, data, or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the **Regulatory Authority**.
* **Politically Exposed Persons (PEPs):** Individuals who are or have been entrusted with prominent public functions in a foreign country.
* **Regulated Entities (REs):** All Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs / CCBs) and any other entity licensed under Section 22 of Banking Regulation Act, 1949 (referred to as ‘banks”), All India Financial Institutions (AIFIs), All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs), Asset Reconstruction Companies (ARCs), All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers), All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.
* **Shell Bank:** A bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country.
* **Wire transfer:** A transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through a **Regulated Entity** by electronic means to make an amount of money available to a beneficiary person at a **Regulated Entity**.
  + **Domestic and cross-border wire transfer:** Domestic when originator and beneficiary are in the same country; cross-border when in different countries.
  + **Correspondent banking:** Provision of banking services by one bank (correspondent bank) to another bank (respondent bank).
  + **Payable-through accounts:** Correspondent accounts used directly by third parties to transact business on their own behalf.
  + **V-CIP (alternate method):** An alternate method of customer identification with facial recognition and customer due diligence by an authorized official of the **Regulated Entity** by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer.
  + **Batch transfer:** A transfer comprised of a number of individual wire transfers sent to the same financial institution.
  + **Beneficiary:** Natural or legal person identified by the originator as the receiver of the wire transfer.
  + **Beneficiary Bank:** A financial institution that receives the wire transfer and makes funds available to the beneficiary.
  + **Cover Payment:** Combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with funding instruction routed through one or more intermediary financial institutions.
  + **Financial Institution (Wire-transfer context):** As ascribed in FATF Recommendations.
  + **Intermediary Bank:** A financial institution or entity that handles an intermediary element of the wire transfer in a serial or cover payment chain.
  + **Ordering Bank:** The financial institution which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.
  + **Originator:** The account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.
  + **Serial Payment:** A direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions.
  + **Straight-through Processing:** Payment transactions conducted electronically without manual intervention.
  + **Unique transaction reference number:** A combination of letters, numbers, or symbols determined by the payment service provider.

All other expressions shall have the same meaning as assigned under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder, or as used in commercial parlance.

**4. General**

* The KYC policy of the **Regulated Entity** shall be duly approved by its Board of Directors or any committee to which power has been delegated.
* The **Regulated Entity** shall ensure that a group-wide policy is implemented for obligations under Chapter IV of the Prevention of Money-laundering Act, 2002. This policy serves as the base document for implementing group-wide programs against money laundering and terror financing, including sharing information for client due diligence and risk management, with safeguards on confidentiality.
* The **Regulated Entity's** policy framework should ensure compliance with PML Act/Rules, regulatory instructions, and provide a bulwark against threats from money laundering, terrorist financing, proliferation financing, and other related risks. Best international practices, considering FATF standards and guidance notes, may also be adopted.

**5. Key Elements of KYC Policy**

The KYC policy shall include the following four key elements:

* Customer Acceptance Policy
* Risk Management
* Customer Identification Procedures (CIP)
* Monitoring of Transactions

**5A. Money Laundering and Terrorist Financing Risk Assessment**

* The **Regulated Entity** will carry out Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment periodically to identify, assess, and mitigate risks for clients, countries or geographic areas, products, services, transactions, or delivery channels. The assessment will consider all relevant risk factors to determine the overall risk level and appropriate mitigation.
* The **Regulated Entity** will take cognizance of overall sector-specific vulnerabilities shared by the **Regulator**/supervisor.
* The risk assessment will be properly documented and proportionate to the nature, size, geographical presence, complexity of activities/structure of the **Regulated Entity**. The periodicity will be determined by the Board or a delegated committee, aligned with the risk assessment outcome.

**6. Designated Director**

* A "Designated Director" is a person designated by the **Regulated Entity** to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules, nominated by the Board.
* The name, designation, address, and contact details of the Designated Director shall be communicated to the **Financial Intelligence Unit** and the **Regulatory Authority**. The Principal Officer shall not be nominated as the 'Designated Director'.
* The Director, **Financial Intelligence Unit** can take appropriate action, including imposing a monetary penalty, for failure to comply with KYC/AML/CFT obligations.

**7. Principal Officer**

* The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.
* The name, designation, address, and contact details of the Principal Officer shall be communicated to the **Financial Intelligence Unit** and the **Regulatory Authority**.

**8. Compliance of KYC Policy**

* The **Regulated Entity** will ensure compliance with KYC Policy by specifying who constitutes 'Senior Management' for KYC compliance, allocating responsibility for effective implementation, and submitting quarterly audit notes and compliance to the Audit Committee.
* Decision-making functions for determining KYC norm compliance should not be outsourced.
* The Compliance Function is responsible for evaluating and ensuring adherence to KYC policies and procedures and independent evaluation of the entity's own KYC/AML/CFT policies against legal and regulatory requirements.
* The Board of Directors is responsible for ensuring an effective KYC program, establishing appropriate procedures, and ensuring their effective implementation for full compliance with KYC/AML/CFT guidelines of the **Regulatory Authority**.
* The machinery for implementing the KYC Programme includes:
  + **Board of Directors:** Formulating KYC/AML policies and providing direction and advice on compliance.
  + **Audit Committee of the Board:** Oversight of KYC/AML Compliance, review of inspection reports, and identification of compliance threats.
  + **Designated Director:** Ensures overall compliance with PML Act obligations, oversees policy implementation, and liaises with the **Financial Intelligence Unit**.
  + **AML Principal Officer (MLRO):** Monitors policy implementation, liaises with law enforcement agencies, ensures submission of periodical reports, oversees timely submission of reports to the **Financial Intelligence Unit** (CTR, STR, CCR, NTR, Cross Border Wire transfers >5 lacs), formulates systems, procedures, and controls in KYC/AML, devises procedures for risk profiles, assesses risk in dealings, and conducts staff training.
  + **Relevant Departments/Functions within the Entity:** May include functions like transaction monitoring through AML applications, maintenance and development of AML applications, timely submission of reports, KYC/AML inspection reports, and staff training.
  + **Inspection & Vigilance Department:** Conducting regular, concurrent, and special KYC audits to verify compliance and submit quarterly audit notes.
  + **Regional Offices:** Oversight of KYC/AML guidelines compliance by branches and follow-up on rectification of deficiencies.
  + **Centralized Processing Centre:** For implementing centralized processing for KYC.
* **Additional measures for KYC documents:** The **Regulated Entity** shall ensure that KYC documents are available as per current CDD standards, even if no information change, and if validity has expired, undertake KYC process equivalent to new customer onboarding. PAN details, if available, must be verified from the issuing authority database during periodic updation. Acknowledgment must be provided to the customer for received documents for updation.

**9. Customer Acceptance Policy**

(Details generally included in this section would cover principles for accepting customers, such as ensuring legitimate source of funds, not opening accounts for anonymous or fictitious names, and risk categorization.)

**10. Customer Identification Procedures (CIP)**

(Details generally included in this section would cover the process of identifying and verifying the identity of customers at the time of opening an account or conducting transactions.)

**11. On-going Due Diligence and Monitoring of Transactions**

* The **Regulated Entity** will give special attention to business relationships and transactions with persons from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements. This does not preclude legitimate trade and business transactions.
* The background and purpose of such transactions shall be examined, and written findings with all documents retained and made available to the **Regulatory Authority**/other relevant authorities upon request.

**12. Record Management**

* Records relating to ongoing investigations or transactions subject to disclosure should be retained until the case is confirmed closed.
* Wherever practicable, the **Regulated Entity** is required to seek and retain relevant identification documents for all such transactions and report suspicious transactions.

**13. Reporting Requirements to Financial Intelligence Unit - India**

(This section would detail the types of reports and the procedures for submitting them to the Financial Intelligence Unit.)

**14. Obligations under Specific Acts**

* **Unlawful Activities (Prevention) (UAPA) Act, 1967:** The **Regulated Entity** must comply with obligations under this Act, including not processing transactions of designated persons and entities.
* **Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):** (This section would detail specific obligations under this Act.)

**15. Sanctions List of Designated Individuals and Entities**

(This section would cover the procedures for checking and adhering to sanctions lists.)

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

(This section would detail enhanced due diligence measures for such jurisdictions.)

**17. Secrecy Obligations and Sharing of Information**

* The **Regulated Entity** shall maintain secrecy regarding customer information arising from the contractual relationship.
* Information collected for account opening shall be confidential and not divulged for cross-selling or other purposes without express customer permission.
* When considering requests for data/information from Government and other agencies, the **Regulated Entity** must ensure the information sought does not violate banking secrecy laws.
* Exceptions to secrecy include disclosures under compulsion of law, where there is a public duty to disclose, where the **Regulated Entity's** interest requires disclosure, or with the express or implied consent of the customer.

**18. Compliance with Foreign Contribution (Regulation) Act, 2010**

The **Regulated Entity** shall ensure adherence to the provisions of the Foreign Contribution (Regulation) Act, 2010 and its Rules, and any instructions/communications from the **Regulatory Authority** based on advice from the Ministry of Home Affairs.

**19. CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)**

* The **Central Registry** has been authorized to act as the CKYCR.
* The **Regulated Entity** shall capture customer’s KYC records and upload to CKYCR within 10 days of commencing an account-based relationship.
* Operational Guidelines for uploading KYC data have been released by the **Central Registry**.
* The **Regulated Entity** shall capture KYC information for sharing with the CKYCR as per the Rules and KYC templates for individuals and legal entities.
* The **Regulated Entity** can obtain KYC records online using the KYC Identifier and should not require the client to submit the same KYC records or additional identification documents unless there is a change in information, the retrieved information is incomplete/not as per current norms, validity period has lapsed, or the **Regulated Entity** deems it necessary for verification, enhanced due diligence, or risk profiling.
* Any updated information obtained from the client during identity verification or on-going due diligence must be furnished to the **Central Registry** within seven days or as notified by the Central Government.
* For offline verification, KYC data and redacted Aadhaar number (last four digits) are relevant.
* During periodic updation, all existing KYC records must be incrementally uploaded as per extant CDD standards, especially for active pension accounts without a "KYC identifier".
* KYC records obtained from the **Central Registry** should only be used for identity or address verification and not transferred to third parties unless authorized by the subscriber, **Pension Fund Regulatory Authority**, or the Director (**Financial Intelligence Unit**).
* For accounts opened before CKYCR operationalization, KYC records must be updated in CKYCR during periodic updation, and accounts migrated to current CDD standards.

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

(This section would detail the obligations related to FATCA and CRS reporting.)

**21. Period for Presenting Payment Instruments**

(This section would detail the rules regarding the presentation of payment instruments.)

**22. Operation of Accounts & Money Mules**

(This section would cover guidelines on account operations and preventing the use of accounts by money mules.)

**23. Collection of Account Payee Cheques**

(This section would detail the procedures for collecting account payee cheques.)

**24. Unique Customer Identification Code (UCIC)**

(This section would detail the requirements for maintaining a UCIC for customers.)

**25. Introduction of New Technologies**

* The **Regulated Entity** shall undertake a risk assessment exercise prior to the use of new or developing technologies for its financial schemes and shall take appropriate measures to manage and mitigate the risks.

**26. Correspondent Banking**

* It shall be ensured that a foreign correspondent institution does not permit its accounts to be used by shell banks.
* **Regulated Entities** shall be cautious with correspondent banks located in jurisdictions with strategic deficiencies or insufficient progress in implementing FATF Recommendations.
* **Regulated Entities** shall ensure that respondent banks have KYC/AML policies and procedures and apply enhanced 'due diligence' for transactions through correspondent accounts.

**27. Wire Transfer**

* All cross-border wire transfers shall be accompanied by accurate, complete, and meaningful originator and beneficiary information, including: name of the originator, originator account number, originator’s address/national identity number/customer identification number/date and place of birth, name of the beneficiary, and beneficiary account number.
* The **Regulated Entity** is prohibited from conducting transactions with designated persons and entities and must ensure they do not process cross-border transactions of such persons/entities.
* Complete originator and beneficiary information relating to wire transfers shall be preserved by the **Regulated Entity** involved in the wire transfer, in accordance with the record management policy.

**28. Issue and Payment of Demand Drafts, etc.**

* Any remittance of funds by way of demand draft, mail/telegraphic transfer/NEFT/IMPS or any other mode and issue of travelers’ cheques for value of rupees fifty thousand and above shall be effected by debit to the customer’s account or against cheques and not against cash payment.
* The name of the purchaser shall be incorporated on the face of the demand draft, pay order, banker’s cheques, etc. issued by the **Regulated Entity**.

**29. Quoting of PAN**

(This section would detail the requirements for quoting Permanent Account Number.)

**30. Selling Third-party Products**

(This section would detail the guidelines for selling third-party products.)

**31. At-par Cheques Facility Availed by Co-operative Banks**

* The ‘at par’ cheques facility offered by commercial banks to co-operative banks shall be monitored and such arrangements reviewed to assess risks including credit and reputational risk. Approval shall be obtained from the Regional office, and necessary document/agreement executed.
* The right to verify records maintained by the customer cooperative banks/societies for compliance with KYC and AML instructions shall be retained by the providing **Regulated Entities**.
* Cooperative Banks shall ensure the ‘at par’ cheques facility is utilized only for their own use, for KYC compliant account-holders (transactions of Rs. 50,000 or more by debit to customer accounts), and for walk-in customers against cash for less than Rs. 50,000 per individual.
* They must maintain records for issuance of ‘at par’ cheques (applicant’s name, account number, beneficiary details, date) and sufficient balances/drawing arrangements.
* ‘At par’ cheques issued must be crossed ‘account payee’ irrespective of the amount.

**32. Issuance of Prepaid Payment Instruments (PPIs)**

PPI issuers shall strictly adhere to instructions issued by the Department of Payment and Settlement System of the **Regulatory Authority** through their Master Direction.

**33. Hiring of Employees and Employee Training**

* An adequate screening mechanism, including a Know Your Employee / Staff policy, shall be an integral part of the personnel recruitment/hiring process.
* The **Regulated Entity** shall endeavor to ensure that staff dealing with KYC/AML/CFT matters have high integrity and ethical standards, good understanding of extant standards, effective communication skills, and ability to keep up with the changing landscape. An environment fostering open communication and high integrity should be developed.
* An on-going employee training program shall be in place to adequately train staff in KYC/AML/CFT policy. The focus of training shall differ for frontline staff, compliance staff, and staff dealing with new customers. Frontline staff shall be specially trained to handle issues arising from lack of customer education.
* The audit function should be properly staffed with adequately trained and well-versed persons in KYC.

**34. PFRDA**

(This section would detail specific guidelines related to the Pension Fund Regulatory and Development Authority, if applicable, for the generalized entity.)