Nestavia Home Finance Private Limited

Know Your Customer (KYC) and Anti-Money Laundering(AML) Policy

+91-44-46065151

Nestavia Home Finance Private Limited
Unit 005 - Cowrks, 2nd Floor, 2nd Wing, Sterling Technopolis, No. 4/293, OMR, Perungudi, Chennai - 600096.

www.nestaviahomefin.com
contactus@nestaviahomefin.com
CIN No. U64920TN2024PTC174499
GST No. 33AAJCN9653N1ZR

Name of the Policy: Know Your Customer (KYC) and Anti-Money Laundering (AML) Policy

Policy Number: KYCAML-03/2026

PREAMBLE

Nestavia Home Finance Private Limited (hereinafter referred to as "the Company" or “Nestavia”) is committed to providing the best possible customer experience through the customer first approach.

The Company recognizes its responsibility to promote good and fair practices by setting minimum standards in dealing with customers and thus has implemented this Know Your Customer (KYC) to establish clear guidelines and processes to establish the identity and address of the Customer and to prevent Nestavia Home Finance (Nestavia) from being used, intentionally or unintentionally, by criminal elements for money laundering activities. This policy is to enable Nestavia to understand the customers and their financial dealings better which in turn help to manage the risks prudently.

This Policy is framed in compliance with the provisions of Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025 **(“RBI KYC Directions”)** (as amended from time to time), Prevention of Money-Laundering Act (PMLA), 2002, Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and all other applicable regulations.

Prepared and Proposed By	Compliance Officer
Reviewed and Recommended By	Managing Director & CEO
Approved By	Board of Directors
Date of Approval	30-Apr-2026

RESPONSIBILITY ASSIGNMENT MATRIX

Responsibility for Implementation	Branch Manager at each location

VERSION CONTROL

Version No.	Date of Approval by Board of Directors	Key Highlights/Changes
1.0	23-Apr-2025	Roll-out of policy
2.0	23-Jul-2025	Inclusion of AML measures
3.0	30-Apr-2026	Updation of policy in line with new RBI KYC Directions

Table of Contents

1. Objectives

This policy is designed to develop a clear Customer Acceptance Policy laying down explicit criteria for identification and acceptance of customers, monitoring their transactions and to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing. The objective is to:

- Establish identity and address of customers
- Understand the nature of the customer's activities
- Monitor transactions for suspicious activity
- Enable Risk-Based Customer Due Diligence (CDD)
- Define Internal Controls and KYC Governance
- Ensure compliance with RBI and PMLA guidelines

2. Regulatory Framework

This policy is framed under the following key regulations:

- Reserve Bank of India (Non-Banking Financial Companies - Know Your Customer) Directions, 2025(updated periodically)
- Prevention of Money Laundering Act (PMLA), 2002 and rules thereunder
- Reserve Bank of India (Housing Finance Companies) Directions, 2025
- Guidance from Financial Intelligence Unit – India (FIU-IND)
- FATF Recommendations

3. Scope

This policy applies to:

- All individual and non-individual customers of the Company both existing and new.
- All products and services offered by the Company (home loans, mortgage loans, construction finance, etc.)
- All employees, authorized representatives and outsourced vendors involved in customer onboarding
- All branches of the Company

4. Definitions

- **Customer**: A person/entity maintaining a business relationship or carrying out a financial transaction with the Company.
- **KYC**: Process of verifying identity and address using OVDs (Officially Valid Documents).
- **CDD**: Customer Due Diligence under PMLA Rules.
- **FIU-IND**: Financial Intelligence Unit – India.
- **PEP**: Politically Exposed Person.
- **STR**: Suspicious Transaction Report.
- **CTR**: Cash Transaction Report.

---

5. Governance and Oversight

5.1 Role of the Board

The Board of Directors shall:

- Approve and periodically review this Policy;
- Ensure adequate systems, controls and resources for AML/KYC compliance;
- Oversee the implementation of Risk Based Approach (RBA) for management of ML/TF risks;
- Review the Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment.

5.2 Senior Management

The Chief Executive Officer (CEO), Chief Business Officer (CBO), Chief Operating Officer (COO), National Credit Head and National Legal Head shall constitute the 'Senior Management' for the purpose of KYC Compliance.

The Senior Management shall be responsible for:

- Effective implementation of this Policy;
- Ensuring staff training and internal controls;
- Reporting material compliance issues to the Board.

5.3 Designated Director

"Designated Director" means a Director designated by the Board of Directors of the Company to ensure overall compliance with the obligations imposed under Chapter IV of the PMLA, 2002.

5.4 Principal Officer

Principal Officer means an official of the Company designated by the Board of Directors/ competent authority as authorized by the Board of Directors, who shall be responsible for:

- Acting as the nodal point for FIU-IND;
- Ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made thereunder, as amended from time to time;
- Ensure timely reporting of STRs, CTRs and STR and reporting of counterfeit notes and all other suspicious transactions to FIU-IND;

5.5 Control Measures

- The Company shall put in place effective Internal Audit System to evaluate the compliance with KYC/AML policies, procedures and legal and regulatory requirements;
- A quarterly notes on KYC/AML compliance shall be submitted to the Audit Committee of the Board.

---

6. Customer Acceptance Policy (CAP)

6.1 The Company shall:

- Accept only those customers whose identity and address can be verified using reliable documents.
- Not open accounts in fictitious/benami names.
- Not accept walk-in customers without proper due diligence.
- Not undertake transaction or account based relationship without following the CDD procedure.
- Not open accounts where the company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
- Define circumstances under which a customer may be refused onboarding (e.g., blacklisted entities, PEPs with adverse media).
- Obtain **PAN** and Aadhaar as per regulatory guidance.
- Verify the digital signatures of customers, where applicable, as per the provisions of the Information Technology Act, 2002

6.2 Customer acting behalf of another person/entity:

Where a customer is acting on behalf of another person, the Company shall ensure that both the person acting (customer/representative) and the person on whose behalf the customer is acting (principal/beneficial owner) are properly identified, verified, and risk-assessed, in accordance with applicable KYC Directions and the Prevention of Money-laundering framework.

Permitted Circumstances:

- Beneficial Ownership / Agency Relationships
- Power of Attorney / Mandate / Letter of Authority
- Authorised Signatory of a Juridical Person
- Guardian of a Minor
- Trustee, Executor, Administrator or Court-Appointed Representative

6.3 The Company shall not accept customers whose name is appearing in:

- the lists of individuals and entities ('ISIL (Da'esh) & Al-Qaida Sanctions List' and 'Taliban Sanctions List'), in terms of section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC).
- the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time.
- the designated lists available on the portal of FIU-IND.
- the designated lists under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005).
- the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities ', as available at https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm.

---

7. Customer Identification Procedure (CIP)

The Company shall identify the customer using:

a) For Individuals:

- Aadhaar (voluntary) / Voter ID / Passport / Driving Licence / NREGA Job Card (with photo)
- PAN (mandatory under PMLA)
- Recent photograph

- Proof of address (if not part of OVD)

b) For Non-individuals:

- Certificate of Incorporation
- PAN and GST
- Board Resolution
- Authorized signatories' OVDs and photographs
- Beneficial Ownership declaration as per Rule 9(3) of PMLA Rules

In addition to this, Rule 9 of the PML Rules which provides for the documents/information to be obtained for identifying various types of customers shall also be considered.

CIP will be applied at:

- Onboarding
- At the time of high-value transactions
- Periodically (for risk-based updates)

---

8. Customer Due Diligence

8.1 Customer Due Diligence is a process involving:

(a) Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;

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

(c) Determining whether a customer is acting on behalf of a beneficial owner and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

8.2 CDD shall be carried out at:

- At the time of onboarding
- At the time of high-value transactions or transactions above prescribed thresholds
- When there is a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data
- On an ongoing basis.

Where the Company forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip off the customer, it shall not pursue the CDD process and instead file an STR with FIU-IND.

---

9 Risk Categorisation of Customers

9.1 Customers shall be categorized as:

Category	Examples	KYC Frequency
Low Risk	Salaried individuals, government employees, employees of public sector enterprises, senior citizens etc.	Every 10 years
Medium Risk	SMEs, professionals, unregistered bodies etc.	Every 8 years
High Risk	PEPs, NRIs, trusts, NGOs, charities, cash-intensive businesses etc.	Every 2 years

9.2 Criteria for risk categorization include:

- Nature of business
- Source of funds
- Geographical location
- Reputation

9.3 Periodic review of Risk Categorization

The above risk categorization shall be periodically reviewed in line with Annexure – 2 Customer Risk Categorization Matrix of this policy and Credit Policy of the Company. The periodicity of such review shall be once in every six months. The Company shall establish and apply, if needed, enhanced due diligence measures based on the revies.

---

10. Ongoing Due Diligence

The Company shall:

- Monitor financial transactions to ensure consistency with customer's business and risk profile and their sources of funds/wealth.

- Conduct periodic KYC updates based on risk category.
- Re-verify identity if there's a change in ownership or profile.
- Trigger alerts for unusual or high-risk transactions.
- Screen customers against sanctions lists and other databases to identify any links to money laundering or terrorism financing.
- Require additional CDD measures, when needed.

---

11. Enhanced Due Diligence (EDD)

Applicable for:

- High-risk customers
- Customers from high-risk jurisdictions (FATF list)
- Complex or unusually large transactions.

Measures include:

- obtaining additional identifying information from a wider variety or more robust sources and using the information to inform the individual customer risk assessment
- carrying out additional searches (e.g., verifiable adverse media searches) to inform the individual customer risk assessment
- verifying the source of funds or wealth involved in the business relationship to be satisfied that they do not constitute the proceeds from crime
- seeking additional information from the customer about the purpose and intended nature of the business relationship
- seeking Senior management's approval before onboarding.

---

12. Periodic Updation of KYC

The Company shall adopt a risk-based approach for periodic updation of KYC to ensure the information or data collected under CDD is up-to-date and relevant, particularly where there is high risk.

12.1 KYC information shall be updated:

- Every 2 years for High-risk Customers

- Every 8 years for Medium-risk Customers
- Every 10 years for Low-risk Customers

The customers shall be provided with the facility of updation/ periodic updation of KYC at any branch of the Company.

12.2 Individuals:

- No change in KYC information: self-declaration from the customer in this regard through the registered email-id, mobile number, mobile application, letter, etc.
- Change only in Address: self-declaration from the customer in this regard through the registered email-id, mobile number, mobile application, letter, etc.

  The Company may at its discretion require a copy of OVD or deemed OVD or equivalent documents in this regard.

12.3 Customers other than Individuals:

- No change in KYC information: self-declaration in this regard through the registered email-id, mobile number, mobile application, letter from an official authorised.
  The company shall further ensure that Beneficial Ownership (BO) information available is accurate and shall update the same, if required, to keep it as up-to-date as possible.
- Change in KYC information**:** In case of change in KYC information, the KYC process equivalent to that applicable during onboarding will be undertaken.

12.4 Exceptional measures for KYC updation

The company may, when needed, adopt additional and exceptional measures for KYC updation of existing customers such as:

- requirement of obtaining recent photograph,
- requirement of physical presence of the customer,
- requirement of periodic updation of KYC only in the branch where account is maintained,
- a more frequent periodicity of KYC updation than the minimum specified periodicity.

---

13. KYC Risk Management

The Company shall establish an effective KYC programme with appropriate systems and procedures and ensure their effective implementation. In addition to that it shall formulate a

Risk Based Approach (RBA) by laying down risk assessment principles, methodology and risk mitigation measures.

The Company shall carry out the Internal Risk Assessment (IRA) exercise as per the Internal Risk Assessment Framework enclosed as Annexure III to this policy.

---

14. Records Management

Records to be maintained:

- KYC documents: Minimum 5 years after account closure
- Transaction records: Minimum 5 years from date of transaction
- STR filings and logs: Indefinitely or as per regulatory instructions

---

15. Reporting to FIU-IND

The Company shall:

- File Cash Transaction Reports (CTRs) for transactions > ₹10 lakhs.
- File Suspicious Transaction Reports (STRs) within 7 days of identifying suspicion.
- Nominate a Principal Officer (PO) and a Designated Director for compliance.

---

16. Central KYC Records Registry (CKYCR)

The Company shall use the CKYC Identifier as the primary reference for KYC verification wherever available.

- Fresh KYC documents shall not be sought from customers unless:

  - There is a change in information;
  - KYC data is incomplete or outdated;
  - Enhanced due diligence is required.

- Updated KYC information shall be uploaded to CKYCR within the stipulated regulatory timelines.

---

17. Monitoring of Transactions

Automated transaction monitoring shall be done to:

- Identify suspicious behaviour

- Generate alerts based on thresholds (e.g. cash deposits, multiple loan applications etc.)
- Support STR filings

---

18. Customer Education and Employee Training and Awareness

The Company shall:

- Train employees who interact with Customers to educate them when seeking KYC information
- Conduct annual KYC/AML training for all frontline and compliance staff and educating then on the risks associated with money laundering and terrorism financing, as well as how to identify and report suspicious activity.
- Provide training and awareness programs to employees on risk assessment methodologies, red flags, and compliance requirements
- Provide updated regulatory guidelines and risk trends.
- Test awareness periodically.

---

19. Policy review and amendments

This policy will be reviewed periodically by the Compliance department to ensure compliance with the law, reflect changes in business or regulatory requirements, and enhance its effectiveness. Any amendments will be communicated to customers and training provided to the employees.

---

20. Annexures

- **Annexure I**: List of Officially Valid Documents (OVDs)
- **Annexure II**: Customer Risk Categorization Matrix
- **Annexure III**: Internal Risk Assessment Framework

Annexure - I

List of Officially Valid Documents (OVDs)

For Individuals:

1. Passport
2. Driving Licence
3. Voter's Identity Card issued by the Election Commission of India
4. PAN Card
5. Aadhaar Card (voluntarily submitted and verified through UIDAI authentication, as per Aadhaar Act and RBI guidelines)
6. NREGA Job Card – duly signed by an officer of the State Government
7. Letter issued by the National Population Register containing details of name and address

Note:

- A valid Driving Licence or Passport is one that is not expired.
- Aadhaar can be accepted only if voluntarily submitted by the customer and must be verified via e-KYC or offline verification through UIDAI as permitted.

Proof of Address:

If the OVD submitted by the customer does not contain current address, then the following can be accepted as 'Deemed OVD' for address verification purposes only:

- Utility bill (electricity, water, telephone, gas) – not more than 2 months old
- Property or municipal tax receipt
- Pension or family pension payment orders
- Letter of allotment of accommodation from employer (for government employees)

These are acceptable only for address verification, not for identity.

For Non-Individual Customers:

Entity Type	Required OVDs
Company	- Certificate of Incorporation - PAN Card - Board Resolution - Identification of Authorized Signatories (OVDs of individuals)
Partnership Firm	- Partnership Deed - PAN Card - Registration Certificate (if registered) - OVDs of partners and signatories
Trust	- Registration Certificate - Trust Deed - OVDs of Trustees
Sole Proprietorship	- Business registration certificate - GST/Tax filings - OVD of the proprietor
Unincorporated Association / Body of Individuals	- Resolution of the managing body - Power of attorney/authorization - OVDs of individuals managing the entity

KYC Verification Process Notes:

- All OVDs must be verified via:
    - Original sighting (for offline onboarding)
    - CKYC number (if available)
    - Digital KYC (e-KYC/Aadhaar offline, video KYC)
- Self-attested copies must be retained where applicable.
- Aadhaar usage must comply with Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

Annexure -II

Customer Risk Categorization Matrix

(To be read with Section 9 of the KYC/AML Policy and Credit Policy of the Company)

Risk Parameter	Low Risk	Medium Risk	High Risk
Customer Type	Salaried individuals, government employees, employees of PSUs	Self-employed professionals, MSMEs	Trusts, NGOs, Charitable orgs, Shell companies
Nature of Business / Occupation	Government, PSU, MNCs	Retailers, Contractors, Service Providers	Arms dealers, casinos, real estate brokers, cash-intensive businesses
Geographical Location (residence or business)	Tier 1 to Tier 4 locations, low-risk FATF countries	Tier 5 to Tier 6 locations	High-risk jurisdictions, areas with known crime/terror activity
Source of Funds / Income	Salary in bank, verifiable through official documents	Income from business or rentals with moderate cash transactions	Unverifiable income, heavy cash dealings, foreign remittances with no clear source
Account Activity Profile	Predictable and consistent with known income	Irregular credits/debits, occasional large transactions	Frequent high-value transactions, unexplained credits or third-party transfers
Customer Profile Verification	Verified through official channels, documents in order	Minor discrepancies, require follow-up or clarification	Mismatch in documents, adverse media, negative background check
Politically Exposed Person (PEP)	Not applicable	Family member or close associate of PEP	Foreign PEPs or high-profile domestic PEPs
Type of Product / Loan Applied	Home loan for self-occupied residential unit	LAP (Loan Against Property), resale transactions	Loans involving third-party POA, layered ownership, high-risk projects

Risk Parameter	Low Risk	Medium Risk	High Risk
Delivery Channel	In-person onboarding through branch or approved agents	Digital onboarding with full KYC	Remote onboarding with limited physical verification, third-party sourced customers

Risk Categorisation Outcome:

Risk Score / Profile	Risk Category	KYC Update Frequency
Meets most Low Risk criteria	Low	Once every 10 years
Mix of Low & High or some Medium	Medium	Once every 8 years
Meets multiple High-Risk factors	High	Once every 2 years

Risk category must be reviewed at onboarding and during periodic KYC updates or on the occurrence of trigger events (e.g., change in ownership, suspicious activity, downgrade by risk engine etc.).

Note:

- Final risk classification should be validated by the Compliance Officer or Risk Team.
- Risk categorization should be documented in the Customer Onboarding Form or CRM.
- System-based alerts and flags should be configured to monitor high-risk accounts.

Annexure -III

Internal Risk Assessment Framework on 'Money Laundering (ML) and Terrorist Financing (TF)

Objective:

The Company acknowledges the fact of financial institutions being exposed to Money Laundering (ML)/ Terrorist Financing (TF)/ Proliferation Financing (PF), which may lead to loss of reputation and financial loss, due to the changing business environment, increasing level of complexity in products and adoption of technology. Hence, it is necessary to be aware of the nature and scope of the risks it faces that may lead to ML/TF/PF, the likelihood of them occurring, and the potential impact on the business.

The Company is obligated to comply with ML/TF/PF related legal provisions in terms of Prevention of Money Laundering (PML) Act 2002, PML Rules 2005, Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act), Unlawful Activities (Prevention) Act, 1967 (UAP Act) and other Orders/ Directions of Government and its agencies under these Acts. Also, Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025 dated November 28, 2025, under Para 10, further requires the Company to carry out 'ML and TF Risk Assessment' ('Internal Risk Assessment' or 'IRA') exercise periodically to identify the risks associated.

IRA is a tool to understand the potential sources of such risks and how likely those risks are to occur and determine the impact. The outcome of the assessment activity helps in prioritizing the efforts to manage risks effectively. The activity also facilitates to foster the Risk Based Approach (RBA) which would steer the company to adopt measures according to their risk levels and deploy resources more effectively

Hence it is essential to develop AML/CTF Assessment Program that includes appropriate measures to prevent financial crimes from occurring.

Risk Based Approach (RBA):

The Risk Based Approach (RBA) of the Company enables adoption of a more configurable set of measures in order to deploy their resources more effectively and apply preventive measures that are commensurate with the ML/TF/PF risks posed by the customers.

The Risk Assessment critically involves two levels of assessment one at business level and another at an individual level. The integration of both levels of assessment into a unified assessment program enables the company to adopt an enterprise-wise risk assessment model.

Risk Assessment process:

A. Data Collection:

The risk assessment shall begin with collecting of information on a wide range of variables including both internal data and external data.

a. Internal data:
   - Business processes, nature of products offered
   - Customer data collected during CDD
   - business and customer location
   - Transaction Patterns
   - Technology implied

b. External data:
   - National Risk Assessment report of Government of India
   - Information from Directorate of Enforcement
   - Sanction list published by United Nations Security Council (UNSC) and RBI
   - UNSCR 1718 Sanctions List of Designated Individuals and entities.
   - Information on TF vulnerabilities of specific sectors and products.
   - Guidance & Advisories from government authorities, FIU-IND & RBI
   - FATF reports and research reports from accredited agencies
   - open-source intelligence such as from news articles, market inputs, etc., about products, customers, transactions, etc.

B. Risk Identification:

a. Identification of Inherent Risks:

i. ***Customer Profile:*** Politically Exposed Persons (PEP), individual who has been entrusted with a prominent public function, engaged in a business which involves significant amounts of cash, reluctant or unwilling to provide adequate explanations or documents, customers' source of funds, customers' background like history of financial crimes, control structure of corporate customers (Companies, Trust, Partnership firms etc.), inactive entities, delegation of authority by the applicant or customer for example, the use of powers of attorney, mixed boards and representative offices.

ii. ***Type/Nature of Products/ Services:*** Higher value of loan product, complexity of product, digital products, Customer onboarding through Online mode / app based/non-face-to-face.

Some of the queries with respect to product that may be considered for risk evaluation:

- Does the company accept large cash payments or virtual currency?

- Does the product/service allow for anonymity (i.e. not physically seeing or meeting the actual customer)?
- Does the product/service disguise or conceal the beneficial owner of the customer?
- Does the product/service disguise or conceal the source of wealth or funds of the customer?
- Does the product/service allow payments to, or from third parties?
- Does the product/service commonly involve receipt or payment in cash?
- Does the product/service allow for the movement of funds across borders?
- Does it place funds in customer, nominee or other accounts, where funds are mingled with others' funds?

iii. ***Business Model (complexity of business):*** Models involving dealing through intermediaries or third parties, relying on third parties to conduct CDD.

iv. ***Transaction***: Volume and size of transactions involved while considering the usual activity of the Company and the profile of the customers.

b. Identification of Control Risk Types:

i. ***Geographic areas of service (Target markets):*** Risks include weaker regulatory frameworks, Customers' living in high-risk jurisdictions especially jurisdictions with relatively higher levels of corruption or organised crime, prevalence of bribery and corruption, association with terrorism and TF and /or deficient AML/CFT controls and listed by RBI or FATF.

ii. ***Delivery Channels:*** How your entity delivers products and services are vulnerabilities that your customers, associates or counterparties may attempt to exploit to conduct ML or TF.

iii. ***Involvement of third parties***: Any outsourcing, third party reliance and dependence on unregulated intermediaries for provision of products/ services.

iv. ***Lack of information:*** Ability or lack thereof, to obtain necessary information in case of wire transfers.

v. The internal audit and regulatory observations.

C. Assessment of Risk Factors:

The company shall adopt data-oriented objective approach to ensure absence of any kind of bias in the IRA exercise and quality of data inputs resulting meaningful/ useful outcomes.

The assessment of risk is evaluated based on the following equation:

"Threat + Vulnerability (severity) + Consequence/potential impact = Risk"

In addition, the probability/likelihood of the event shall be considered.

a. Definitions for the different categories of likelihood:
   i. Almost certain: There is a high probability of ML / TF occurring
   ii. Likely: There is a medium probability of ML / TF occurring
   iii. Unlikely: There is a low probability of ML / TF occurring
   iv. Possible: There is a minuscule probability of ML / TF occurring

b. Assessment Team:

The company's officials carrying out this assessment exercise shall be from different functions, having vide range of expertise, as decided by the MD & CEO time to time.

c. Assignment of Weights:

While the standard practice is to assign a score to each risk factor/sub-risk factor, the RBI guideline additionally requires the Company to assign weights based on the contribution of each risk factor to the overall ML/TF risk. This weighted system facilitates to ensure that the risk factors that pose the greatest threat are prioritised.

d. Levelling of Risk based on risk scores:

The weighted inherent risk score for each risk factor/sub-risk factor, as applicable, would be mapped to appropriate risk levels viz., 'High', 'Medium' and 'Low' to arrive at the 'inherent risk level'.

e. Review of Level of Risk:
   - change in the nature of your business relationship with a customer
   - change in transaction patterns
   - changes to a customer's corporate structure or other control structures.
   - changes in external data on ML/TF (FATF reports etc.)

The "Internal Risk Assessment Guidance for Money Laundering/ Terrorist Financing Risks" shall be referred and adopted by the Company, as and when required, for the purpose of Risk Assessment Methodology, Risk classification, Assigning weights to the Risk factors/Sub-risk factors, and Internal Controls measures.

D. Application of Control/Mitigation measures:

Adequate internal controls shall be identified and evaluated to determine their effectiveness in mitigating/ controlling the overall risks post IRA. Internal Controls shall include:

i. Governance and assurance function;

ii. Integrity of staff and compliance culture;

iii. Implementation of policies and procedures, as reviewed from time to time, designed to detect and prevent financial crimes;

iv. KYC/ due diligence;

v. Enhanced Due Diligence (EDD) for high-risk customers;

vi. Transaction Monitoring and controls;

vii. Ongoing monitoring;

viii. Suspicious transaction reporting;

ix. Screening of sanctions lists such as sanctions lists pursuant to UNSC Resolutions 1267(1999), 1373(2001), etc., and freezing of accounts. Factors such as - effectiveness of the name matching in various combinations, frequency of screening, whether applicable to only account-based relationships or transactions also, etc., should be considered.

x. Independent testing/ model validations/ audit;

xi. Record keeping/retention;

xii. Employees Recruitment & Training.

E. Determination of Residual Risk:

Determination of Residual Risk is a process of assessment of remaining risk post implementation of internal controls. Calculating residual risk is essential for determining whether the mitigation controls that are implemented are effective. If the residual risk is too high, the company shall implement additional mitigation controls or adjust the existing controls by strengthening internal controls to reduce the level of risk.

F. Monitoring and Review:

a. Regular monitoring of Risks and incorporation of emerging risks

b. Review of effectiveness of controls and mitigation measures to remain effective and up-to-date with any changes in business or industry.

c. Review and updation of IRA to reflect new products, technologies, business models or emergence of relevant new threats.

G. Documentation:

There will be proper maintaining detailed documentation and audit trails of risk assessment processes, including assumptions, methodologies, and decision-making criteria to ensure transparency and accountability and facilitate internal reviews and regulatory compliance.

H. Periodicity of Risk Assessment:

a. Annually: Assessment Report shall be submitted for the review of Risk Management Committee and Board of Directors.
b. Before offering of new products & services to customers which shall include:

- new designated services
- new ways of delivering existing designated services
- using new technologies to provide designated services
- engaging with a new jurisdiction.