Know Your Customer Norms (KYC)
And Anti Money Laundering (AML) Measures

Namdev Finvest Private Limited

Registered Office:

S-1, S-7-8, SHREE NATH PLAZA, SECOND FLOOR,

NEER SAGAR MARKET, BHANKROTA,

JAIPUR, RAJASTHAN-302026

INDIA

CIN NO: U65921RJ1997PTC047090

Policy Name	**Know Your Customer Norms (KYC) And Anti Money Laundering (AML) Measures**	
Version	**2.0**	
Effective date	**June 2024**	
Prepared and proposed by	**Ms. Sakshi Sharma**	
Approver	**Board of Directors**	**May 2025**

INDEX

1. Introduction

Namdev Finvest Private Limited (NFPL) is a Non-Banking Financial Company having valid Certificate of Registration with Reserve Bank of India vide registration No. B-10.00260 on 20th August 1997 under current RBI classification as NBFC – Non-Deposit taking Asset Finance Company.

It is focused on offering finance to MSME, Two-wheelers, Solar panel loan, Electric Vehicle (EV) loan, EV charging station loan and all kind of light commercial vehicles segment.

2. Objectives

To lay down explicit criteria for acceptance of customers.

- To establish procedures to verify the bona-fide identification of individuals/ non individuals before becoming an account holder/customer.
- To enable the Company to know/understand the customers and their financial dealings better, which in turn would help the Company to manage risks prudently.
- To develop measures for conducting due diligence in respect of customers and reporting of such transactions.
- To comply with applicable laws and regulatory guidelines.
- To take necessary steps to ensure that the relevant staff are adequately trained in KYC/AML procedures.
- To prevent criminal elements from using the Company for money laundering activities.

3. Scope

This policy is applicable to all branches and all other offices of the Company.

Definitions

A "Customer" for the purpose of this policy is defined as:

- A person or an entity that maintains an account and/or has a Business relationship with the Company.
- One on whose behalf the account is maintained i.e. the Beneficial Owner.
- Beneficiaries of transactions conducted by Professional Intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law and
- Any person or entity connected with a financial transaction.

Money laundering

Section 3 of the Prevention of Money Laundering [PML] Act 2002 has defined the "offence of money laundering' as under:

"Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds or crime and projecting it as untainted property shall be guilty of offence of money laundering".

4. Know Your Customer Standards

The revised KYC policy of the Company incorporates the following four elements:

- Customer Acceptance Policy (CAP)
- Customer Identification Procedures (CIP)
- Monitoring of Transactions; and
- Risk Management

1. Customer Acceptance Policy (CAP)

The following Customer Acceptance Policy indicating the criteria for acceptance of customers shall be followed in the Company. The branches shall accept customer strictly in accordance with the said policy:

- The Company will have an elaborate standard for obtaining comprehensive information regarding new customers at the initial stage and that of existing customers over a predetermined period, thereby establishing the Bonafede's of customers opening credit accounts with the Company.
- The Company will lay down/spell clearly the document requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the guidelines issued by Reserve Bank of India from time to time i.e. nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc.
- The Company will not open accounts in the name of anonymous/fictitious/ benami persons.
- The Company will ensure that circumstance in which a customer is permitted to act on behalf of another person/entity will be clearly spelt out in conformity with the established law and practice of banking as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in the fiduciary capacity.
- Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and guidelines issued by Reserve Bank from time to time;
- The company shall not to open an account or close an existing account where the company is unable to apply appropriate customer due diligence measures i.e., the company is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non-cooperation of the customer or non-reliability of the data/information furnished to the company. It shall be necessary to have suitable built-in safeguards to avoid harassment of the customer. For example, decision to close an account shall be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision;
- Circumstances, in which a customer is permitted to act on behalf of another person/entity, shall be clearly spelt out in conformity with the established law and practice of banking as there shall be occasions when an account is operated by a mandate holder or where an account shall be opened by an intermediary in the fiduciary capacity and

- The Company will ensure that before opening a credit account there are adequate checks to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities like individual terrorist or terrorist organizations.
- The company shall prepare a profile for each new customer based on risk categorisation. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence shall depend on the risk perceived by the company. However, while preparing customer profile the company shall take care to seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile shall be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.
- For the purpose of risk categorisation, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, shall be categorised as low risk. Illustrative examples of low risk customers would be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government departments & Government owned companies, regulators and statutory bodies etc. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met. Customers that are likely to pose a higher than average risk to the bank may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Banks may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.
- Examples of customers requiring higher due diligence may include: -
  A. Non-resident customers,
  B. High net worth individuals,
  C. Trusts, charities, NGOs and organizations receiving donations,
  D. Companies having close family shareholding or beneficial ownership,
  E. Firms with 'sleeping partners',
  F. Politically exposed persons (PEPs) of foreign origin,
  G. Non-face to face customers, and
  H. Those with dubious reputation as per public information available, etc.
- Adoption of customer acceptance policy and its implementation shall not become too restrictive and the Company will strive not to inconvenience the general public, especially those who are financially or socially disadvantaged.

2. Customer Identification Procedure (CIP)

Identification is an act of establishing who a person is. In the context of KYC, it means establishing who a person purports to be and will involve identifying the customer and verifying his/her identities by using reliable and independent source documents, data or information. For this purpose, the Company will obtain sufficient information necessary to establish to its satisfaction the identity of each new customer, whether regular or occasional and the purpose of the intended nature of relationship.

Being satisfied means that the Company must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk-based approach is considered necessary to avoid disproportionate cost to Company and a burdensome regime for the customers.

Identity is verified for:

- The named account holder
- Beneficial owner's
- Signatories to an account and
- Intermediate parties.

1. Accounts of Individuals

In case of customers that are natural person the Company will obtain sufficient identification data to verify

(a) The identity of customer

(b) his/her address/ location and

(c) his/her recent photograph. The true identity and bonafide of the existing customers and new potential customers opening credit accounts with the Company and obtaining basic background information would be of paramount importance.

2. Other than individual accounts

For customers that are legal person or entities the Company will

- Verify the legal status of the legal person/entity through proper and relevant documents,
- verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person,
- Understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

Implementation of the KYC norms should not result in denial of services (including opening of credit account) to the public, especially to those, who are financially or socially disadvantaged. The low-income group both in urban and rural areas should not be denied services merely for the reason that they are unable to produce documents to satisfy the Company about their identity and address.

3. Accounts of companies and firms

Branches need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks. Branches should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders. But at least promoters, directors and its executives need to be identified adequately.

4. Accounts of Politically Exposed Persons (PEPs) resident outside India

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Branches should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Branches should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The branches should seek prior approval of their concerned Credit Heads for opening an account in the name of PEP.

5. Accounts of proprietary concerns

Apart from following the extant guidelines on customer identification procedure as applicable to the proprietor, the Company should call for and verify the following documents before opening of accounts in the name of a proprietary concern:

Proof of the name, address and activity of the concern, like registration certificate including udyam registration certificate (in the case of a registered concern), certificate/licence issued by the Municipal authorities under Shop & Establishment Act, sales and income tax returns, CST/VAT certificate, certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities, Licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, registration/licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/Department. the Company may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT, the complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities and utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern as required documents for opening of bank accounts of proprietary concerns.

Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.

Obtaining Guarantor on credit facilities

The Company generally insists on "Guarantee" by a known person (who becomes guarantor to a particular credit facility). Obtaining Guarantee from a known person is a process of ascertaining the identity of a person and his acceptability for establishing business relationship and verifying the true identity of the intending customer before opening a credit account. Further, Guarantor also acts as an introducer of the customer to the Company for the credit facilities.

Liabilities of the Guarantor

Guarantor is legally responsible to the Company for the repayment of the credit facilities by the customer and is expected to be in a position to identify/trace the account holder in case of need.

Procedure for providing Guarantee

The Guarantor will be required to sign on the agreement entered into with the Customer at various places provided in the loan agreement form.

The Guarantor will be normally required to visit the Company's branch for signing the agreement. However, this need not be compulsory.

Closure of accounts

Where the company is unable to apply appropriate KYC measures due to no furnishing of information and /or non-cooperation by the customer, the company will consider closing the account or terminating the banking/business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions will be taken at a reasonably senior level.

3. Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring shall depend on the risk sensitivity attached with the client. The Company shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

The Company shall prescribe threshold limits for a particular category of clients and pay particular attention to the transactions which exceed these limits, Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer would particularly attract the attention of the Company. Further, there are no operative accounts where in the need for fixing the threshold limits for individual transactions and aggregate is more relevant and necessary. All the company's loans are EMI based loans on all categories of borrowers. Hence the transactions with the company are purely shall be restricted to the EMI payable over the tenor of the loan. Hence while the threshold limit for transactional basis is restricted to the EMI payable, the threshold for turnover shall be restricted to the aggregate EMIs payable year after year. No other transactions what so ever nature other than repayment of loan with interest is carried out by the customer with the company.

The permanent correct address shall mean the address at which a person usually resides and can be taken as the address as mentioned in a utility bill or any other document accepted by the company for verification of the address of the customer. In case utility bill is not in the name of the customer but is close relative: wife, son, daughter and parents etc. who live with their husband, father/mother and son, the company shall obtain an identity document and a utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) is a relative and is staying with him/her. The company shall use any supplementary evidence such as a letter received through post for further verification of the address. While issuing operational instructions to the branches on the subject, company shall keep in mind the spirit of instructions issue d by the Reserve Bank and avoid undue hardships to individuals who are, otherwise, classified as low risk customers.

The company shall put in place a system of periodical review of risk categorisation of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Review of risk categorisation of customers shall be carried out at a periodicity of not less than once in six months. The company shall also introduce a system of periodical updating of customer identification data (including photograph/s) after the account is opened. The periodicity of such updating shall not be less than once in five years in case of low-risk category customers and not less than once in two years in case of high and medium risk categories.

4. Risk Management

The Board of Directors of the Company shall ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It shall cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility would be explicitly allocated within the Company for ensuring that the Company's policies and procedures are implemented effectively. The Company shall, in consultation with their Board, devise procedures for creating Risk Profiles of their existing and new customers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.

The Company has an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements shall have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

In terms of PMLA Rules, suspicious transaction shall include inter alia transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. The company, therefore, shall develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority.

As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), is circulated by Reserve Bank, the company shall ensure to update the consolidated list of individuals and entities as circulated by Reserve Bank. The company shall, before opening any new account, ensure that the name/s of the proposed customer does not appear (screening) in the list of RBI, World Bank, UN, EU and OFAC sanctions lists and International Finance Corporation exclusion list. Further, the company shall scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall be immediately be intimated to RBI and FIU-IND. KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the financial channels. Adequate screening mechanism shall be put in place by the company as an integral part of recruitment/hiring process of personnel.

5. Cash and Suspicious Transaction Reports

A. Cash Transaction Report (CTR)

In terms of the Prevention of Money Laundering Act (PMLA), 2002, the company shall report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND).

For determining integrally connected cash transactions, NBFCs shall take into account all individual cash transactions in an account during a calendar month, where either debit or credit summation, computed separately, exceeds or equal to Rupees Ten lakh during the month.

CTR should contain only the transactions carried out by the company on behalf of their clients/customers excluding transactions between the internal accounts of the bank. A summary of cash transaction report for the bank as a whole should be compiled by the Principal Officer of the company every month in physical form as per the format specified. The summary should be signed by the Principal Officer and submitted to FIU-India.

B. Suspicious Transaction Reports (STR)

The Suspicious Transaction Report (STR) should be furnished 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 of the company shall record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from the company or any other branch office. Such report will be made available to the competent authorities on request.

Further the company shall not put any restrictions on operations in the accounts where an STR has been made. The company and its employees shall keep the fact of furnishing of STR strictly confidential, as required under PML Rules. It should be ensured that there is no tipping off to the customer at any level.

Maintenance of records of transactions/Information to be preserved/Maintenance and preservation of records/Cash and Suspicious transactions reporting to Financial Intelligence Unit- India (FIU-IND)

Government of India, Ministry of Finance, Department of Revenue, vide its notification dated July 1, 2005 in the Gazette of India, has notified the Rules under the Prevention of Money Laundering Act (PMLA), 2002. In terms of the said Rules, the provisions of PMLA, 2002 came into effect from July 1, 2005. Section 12 of the PMLA, 2002 casts certain obligations on the banking companies in regard to preservation and reporting of customer account information.

(i) Maintenance of records of transactions

The company shall maintain the proper record of transactions prescribed under Rule 3 of PML Rules, 2005, as mentioned below:

- all cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency;
- all series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rupees Ten Lakh;
- all transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency;
- all cash transactions, where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transaction and
- All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

(ii) Information to be preserved

The company will maintain all necessary information in respect of transactions referred to in Rule 3 to permit reconstruction of individual transaction, including the following information:

- the nature of the transactions;
- the amount of the transaction and the currency in which it was denominated;
- the date on which the transaction was conducted; and
- the parties to the transaction

(iii) Maintenance and Preservation of Records

The company will maintain the records containing information of all transactions including the records of transactions detailed in Rule 3 above. The company should also take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities

Further, in terms of PML Amendment Act 2012 notified on February 15, 2013, the company should maintain for at least five years from the date of transaction between the bank and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

The company should ensure that records pertaining to the identification of the customer and his address (e.g., copies of documents like passports, identity cards, driving licenses, PAN card, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended as required under Rule 10 of the Rules. The identification records and transaction data should be made available to the competent authorities upon request.

(iv) Reporting to Financial Intelligence Unit – India

In terms of the PMLA Rules, the company will report information relating to cash and suspicious transactions and all transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address:

Director, FIU-IND,
Financial Intelligence Unit-India, 6th Floor,
Hotel Samrat, Chanakyapuri,
New Delhi -110021
Website - http://fiuindia.gov.in/

6. Customer Education/Employee's Training/Employee's Hiring

a) Customer Education

The Company recognizes the need to spread awareness on KYC, Anti Money Laundering measures and the rationale behind them amongst the customers and shall take suitable steps for the purpose. Also provide declaration for compliance of Anti Money laundering.

The front desk staffs need to be specially trained to handle such situations while dealing with customers.

b) Employees' Training

The company must have an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Requirements have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

c) List Compilation

Employees must compile with list of UK and UN sanction list

d) Appointment of Principal Officer:

The Company shall designate any senior management or equivalent (know as Chief Executive officer, Chief Compliance Officer, Company Secretary, Chief Financial Officer, Chief Treasury Officer or any other equivalent) or any director as 'Principal Officer' (PO) who shall be located at the Corporate office and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. However, in absence of Company Secretary, the Chief Financial Officer of the Company shall be considered as the principal officer of the Company until a Company Secretary is appointed. The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.

e) Appointment of Designated Director:

The Board of Directors shall nominate a "Designated Director" to ensure compliance with the obligations prescribed by the PMLA and the Rules there under. The "Designated Director" can be a person who holds the position of senior management or equivalent. Accordingly, the Chief Executive Officer of the Company will be nominated as Designated Director by the Board of the Company. However, in absence of the Chief Executive Officer, the Managing Director of the Company shall be considered as the Designated Director of the Company until a Chief Executive Officer is appointed. It shall be ensured that the Principal Officer is not nominated as the "Designated Director". The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

List of integrity red flags at each stage from client onboarding, credit underwriting and loan payment.

A. Client Onboarding

1. **General Red Flags**
   - Inconsistent or false information provided during the onboarding process
   - Customer reluctance to provide necessary documentation for due diligence
2. **Corporate Clients**
   - Lack of transparency regarding beneficial ownership
   - Presence in high-risk jurisdictions with weak regulatory framework
3. **Individual Clients**
   - Politically exposed status with unclear sources of wealth
   - Multiple accounts opened under variations of the same identity

B. Credit Underwriting

1. **Financial Statements**
   - Unexplained discrepancies or sudden changes in financial statement
   - Overstated assets or understated liabilities

2. **Collateral Evaluation**
   - Valuation discrepancies in the collateral provided
   - Multiple loans secured by the same collateral
3. **Industry Specific red flags**
   - For real estate: Frequent property flips or unexplained increases in property values.
   - For manufacturing: Unusual changes in inventory levels

C. Loan Payment

1. **Payment patterns**
   - Consistently late or irregular payments
   - Abrupt changes in payment behavior without a clear explanation
2. **Financial Stress Indicators**
   - Frequent overdrafts and insufficient fund notifications
   - Consistent use of credit to meet financial obligations
3. **Industry Specific Red flags**
   - For agriculture - Crop failure affecting the borrower's ability to repay
   - For retail - Rapid decline in sales impacting cash flow

D. Monitoring And Ongoing Due Diligence

1. **Unusual Transactions**
   - Large, unexplained transactions inconsistent with the customer's profile
   - Frequent movement of funds between accounts
2. **Legal and Regulatory compliance**
   - Regulatory violations or legal actions against the customer
   - Changes in the customer's risk profile due to legal issues
3. **Behavioral Red flags**
   - Employee complaints or whistleblowing regarding unethical practices

<u>Guidelines for employees on identifying and assessing red flags</u>

A. Client Onboarding

1. **Verification of information**
   - Employees should verify all provided information for accuracy and consistency
   - Cross-check client-provided data against external sources to identify discrepancies
2. **Beneficial Ownership Scrutiny**
   - Conduct due diligence to understand beneficial ownership structures
   - Identify and investigate any complex ownership hierarchies
3. **High Risk Jurisdictions**
   - Be cautious when dealing with clients operating in or having connections to high-risk jurisdiction
   - Implement enhanced due diligence procedures for such clients

B. Credit Underwriting

1. **Financial Statement Analysis**
   - Scrutinize financial statements for inconsistencies or sudden change
   - Conduct ratio analysis to assess financial health
2. **Collateral Examination**
   - Verify the valuation of collateral independently
   - Implement periodic assessments to ensure the collateral's ongoing value
3. **Industry Specific Analysis**
   - Understand industry-specific risk factors
   - Tailor credit assessments based on industry characteristics

C. Loan Payment

1. **Payment pattern Monitoring**
   - Regularly monitor payment patterns and deviations
   - Investigate and communicate with clients regarding any irregularities
2. **Financial Stress indicators**
   - Watch for signs of financial distress, such as overdrafts or credit dependence
   - Implement proactive measures for clients facing financial challenges
3. **Industry Specific Awarness**
   - Stay informed about industry-specific factors affecting clients
   - Adjust expectations and risk management strategies based on industry dynamics

D. Monitoring And Ongoing Due Diligence

1. **Transaction Monitoring**
   - Implement robust transaction monitoring systems
   - Investigate any unusual or large transactions promptly
2. **Regulatory Compliance**
   - Stay updated on regulatory changes and compliance requirements
   - Regularly audit client records for adherence to regulatory standards
3. **Behavioral Red flags**
   - Encourage employees to report any observed unethical behavior promptly
   - Establish a mechanism for anonymous reporting to encourage transparency

E. Training And Communication

1. **Regular Training Programs**
   - Conduct regular training sessions on red flag identification and assessment
   - Keep employees informed about evolving risks and compliance standards
2. **Communication Channels**
   - Establish open communication channels for employees to report concerns
   - Promote a culture of accountability and ethical behavior

3. **Cross Functional Collaboration**
    - Encourage collaboration between departments to share insights and observations
    - Foster a team approach to risk management

Escalation procedures and decision-making criteria

A. Escalation Procedures

1. **Immediate Supervisor Notification**
    - Employees should report identified red flags to their immediate supervisor promptly
    - Supervisors are responsible for initial assessment and may need to gather additional information
2. **Department Head Involvement**
    - If the red flag requires further investigation, the matter should be escalated to the department head
    - Department heads may consult with relevant stakeholders to assess the severity and potential impact
3. **Cross0Functional Involvement**
    - For complex issues that cut across departments, encourage cross-functional collaboration
    - Establish a designated team to collectively assess and address high-risk situations
4. **Executive Management Involvement**
    - Red flags deemed significant or high-risk should be escalated to executive management
    - Executive management may conduct a thorough review and decide on appropriate actions
5. **Board or regulatory Reporting**
    - In cases involving serious legal or regulatory implications, consider reporting to the board or relevant regulatory bodies
    - Legal counsel may be involved to guide the process and ensure compliance

B. Decision Making Criteria

1. **Risk Severity**
    - Assess the severity of the red flag in terms of potential financial, legal, or reputational impact
    - Establish criteria for categorizing risks into low, moderate, high, or critical level

2. **Impact on stakeholders**
    - Evaluate the potential impact on various stakeholders, including clients, employees, and shareholders
    - Consider the broader consequences of the red flag for the organization's relationships
3. **Relevance to core business**
    - Consider whether the red flag directly impacts the core business functions or strategic objectives
    - Assess the alignment with the organization's mission and values

4. **Regulatory Compliance**
   - Evaluate the red flag in terms of compliance with relevant laws and regulations
   - Ensure that decision-making aligns with legal and regulatory requirements
5. **Repeat incidents**
   - Assess whether the red flag represents a one-time occurrence or a recurring issue
   - Repeated incidents may require more rigorous intervention and systemic changes
6. **Mitigation Options**
   - Consider the availability and effectiveness of mitigation options
   - Evaluate the feasibility and impact of implementing corrective measures
7. **Stakeholders Communication**
   - Determine the necessity and timing of communication with stakeholders
   - Establish criteria for transparent and timely communication based on the red flag's significance
8. **Legal Counsel Involvement**
   - Involve legal counsel when legal implications are significant
   - Obtain legal guidance on decision-making, especially when regulatory compliance is at stake

C. Documentation And Continues Improvement

1. **Documentation Practices**
   - Document all steps taken, assessments made, and decisions reached during the escalation process
   - Maintain a clear record for auditing, compliance, and continuous improvement
2. **Post incident Analysis**
   - Conduct post-incident analysis to assess the effectiveness of the decision-making process
   - Identify areas for improvement and implement changes to prevent similar occurrences
3. **Training and Awareness**
   - Use insights from red flag incidents to enhance employee training and awareness programs
   - Foster a culture of continuous improvement and proactive risk management