

The Rajasthan State Co-Operative Bank Ltd., Jaipur.

Resolved to implement the "Know your customer policy" framed by the RSCB on the basis of guidelines issued by Reserve Bank of India under section 35-H of the Banking Regulation Act. 1949, on the recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering Standard (AML Std.) For "Combating Financing of Terrorism, on the basis of paper issued on customer due diligence (CDD) for banks by Basel committee on banking supervision objective, the purpose of which is to prevent Banks/Branches from being used intentionally or unintentionally, by criminals for money laundering activities. "The Know your customer policy" is as follows: -

1. This policy has been framed on the basis of guidelines issued by Reserve Bank of India under section 35-H of the Banking Regulation Act 1949 (As applicable to societies) and any contravention or non compliance with the same may attract penalties under the relevant Act.
2. The policy has been framed on the basis of Know Your Customer guidelines circulated by the Reserve Bank of India On the recommendations made by the "Financial Action Task Force"(FATF) on "Anti Money Laundering Standard" (AML Std.) for "Combating Financing of Terrorism" i.e. standards that have become the international benchmark for framing policies on Anti Money Laundering and Combating Financing of Terrorism. Compliance with these standards by Banks/Financial institutions and the country have become necessary for international financial relationship guidelines based on the recommendations of Financial Action Task Force and paper issued on Customer Due Diligence (CDD) for Banks by Basel Committee on Banking Supervision objective. The objective of framing of this Know Your Customer Policy is to prevent banks/branches from being used, intentionally or unintentionally by criminals for money laundering activities. KYC procedures also enable Banks / Branches to Know and

understand their customers and to lead to dealing better which in turn help them manage their risks prudently.

This know your customer policy incorporates the following Four Key Elements:-

- A Customer Acceptance Policy (CAP)
- B Customer identification –Procedure (CIP)
- C Monitoring of Transactions (MOT)
- D Risk Management (RM)

Definition of a customer for the purpose of KYC-Policy: -

- (1) A Customer is defined as a person or entity that maintains an account and/or has a relationship with the bank.
- (2) A Customer is a person or entity on whose behalf the account is maintained (i.e. the beneficial owner).
- (3) Beneficiaries of transactions conducted by professional intermediaries such as stock brokers, chartered Accountants, Solicitors etc. as permitted under the law.
- (4) Any person or entity connected with a financial transaction which can pose significant reputational or other threat to bank, say a wire transfer or issue of a high value demand draft as a single transaction.

Customer Acceptance Policy(CAP):-

There exists a well defined relationship between banker & Customers but in order to manage the risks of this relationship prudentially, the banks/branches should ensure that: -

- (1) No account is opened in anonymous or fictitious/ benami names.
- (2) Customers are categorized in to the following categories:

- | | |
|-------------------------------------------------------------------------------------------------------------|----------------|
| a. Low Risk Customers- | Level I risk |
| b. Medium risk Customers- | Level II risk |
| c. High Risk Customer- | Level III risk |
| d. Customers requiring very high level
Of monitoring of accounts e.g. Politically
Exposed persons PEP | Level IV Risk |

Definition of politically exposed persons:

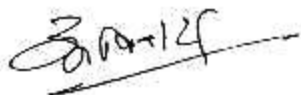
(PEPs)- residing out side India: - Politically Exposed Persons are defined as individuals who are or have been entrusted with prominent public Functions by the country e.g. Heads of State or of Government, Senior Politicians, Senior Government/ Judicial /Military officers executives of State owned Corporations, important political party officials etc., Banks / Branches should gather sufficient information regarding any persons/customer of this category intending to establish a relationship and check all the information available about the person in the Public Domain:- Banks should verify the identity of the person and seek information about the sources before accepting the PEP as a customer. The decision to open an account for PEP should be taken at the senior most level of the branch i.e. the Branch Manager. Banks/branches should also subject such accounts to enhance on an ongoing basis. The above norms may also be applied to the accounts of the family members & close relatives of PEP.

- 3 Banks/Branches should ensure proper documentation and collect sufficient information regarding different categories of customer depending on perceived risk and keeping in mind the requirements of PML Act 2002 and guidelines issued by RBI/NABARD from time to time.

- 4 Bank/Branches should not open an account or close an existing account where the bank is unable to apply appropriate Customer Due Diligence measures i.e. bank/branch is unable to verify the identity and /or obtain documents required as per the risk categorization due to non cooperation of the customer or non-reliability of the data/information furnished to, the bank/branch may however, be necessary to have suitable built in safe guards to avoid harassment of the customer. For this, the decision to close an account should be taken at a reasonably high level after giving due notice to the customer, citing the reason for such a decision.
- 5 Circumstances in which a customer is permitted to act on behalf of another person/entity should be clearly inconformity with the established law and practice of banking, as there could be occasions when an account holder by mandate holder or where an account may be opened by an intermediary in a fiduciary capacity.
- 6 Necessary checks should be effected before opening a new account so as to ensure that the identity of the customer does not resemble/match/overlap with any person with known criminal background or with banned entities such as terrorists or terrorist organization etc.

Categorisation of customer/preparation of profile.

Banks/Branches should prepare a profile for each new customer based on risk categorization. The customer profile information relating to customer's identity social / financial status, nature of business activity information about business and their location etc. The nature and extent of due diligence will depend on the risk perceived however, while preparing customer profile banks should take care to seek only such information from the customer, which is relevant to the risk category and is not intrusive. The



customer profile will be confidential document and data therein should not be divulged for cross selling or any other purposes.

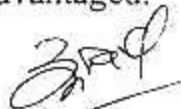
Risk categorization & Risk Management: on the basis of risk profile the customers by and large should be categorized as follows:

Low Risk Customers: Individuals (Other than High net worth Individuals) and entities whose identity and wealth can easily be identified and transactions in whose accounts by and large conform to the known sources of income and can be categorized as low risk. Illustrative examples of low risk customers could be salaried employees whose salary source is well defined and people belonging to lower economic strata of the society whose accounts show small balances. In such cases, only one basic requirement of verifying the identity of the customer are to be met.

Medium Risk Customers: Customers that are likely to pose a higher than average risk to the bank may be categorized as medium risk customers, depending on customers background, nature and location of activity, country of origin, sources of funds and client profile etc.

High Risk Customers: Banks/Branches should apply a intensive "due diligence" for customer specially those whose sources of funds are unknown not revealed/doubtful. This type of customers can be termed as "High Risk Customers". They include (a) non resident customers (b) high Net worth individuals (c) Trusts, charities, N.G.Os and organizations receiving donations (d) companies having close family beneficial ownerships (e) firms with sleeping partners (f) politically exposed persons (PEPS) OF FOREIGN ORIGIN (g) persons of dubious reputation, as per public information available.

Always bear in mind that adoption of customer acceptance policy and it's implementation should not be restrictive and must not result in denial of banking service to general public, especially to those, who are socially disadvantaged.



Customer Identification procedure: Banker's should always use customers identification procedure necessarily:-

- (1) Before establishing a Banker- Customer relationship.
- (2) Carrying out a financial transaction or
- (3) When there is a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data, here identification means identifying the customer and verifying his/her identity by using reliable, independent source data or information.
- (4) Banks/Branches should obtain sufficient information necessary to establish, to their satisfaction, the identity of new customer whether regular or occasional and the purpose of the intended nature of the banking relationship. The Bank/Branches should be able to satisfy the competent authority that due diligence was observed based on the profile of the customer in compliance with the extant guidelines in place. Such risk-based approach is considered necessary to avoid disproportionate cost to banks and a burdensome regime for the customers. Besides risk perception the information/documents required should also depend on the type of customer (individual, Corporate etc.)
- (5) For customers who are natural persons the banks/branches should obtain sufficient identification data to verify the identity of the customer's address/location and also his recent photograph.
- (6) For customers who are legal persons or entities, banks/branches should:-
 - (a) Ascertain the legal status of the legal person/entity through proper and relevant documents,



- (b) Verify that any person pursuing on behalf of the legal person /entity is so authorized, identify, and verify the identity of that person.
- (c) Understand ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal entity/person.

Customer identification requirements in respect of a few typical cases especially, legal persons requiring element of caution are given in Annexure I for guidance to banks/branches. Banks/Branches may however, use their own experience of dealing with such persons, normal bankers, prudence and legal requirement together with well established banking practices. If, the bank/branch decides to accept such accounts in terms of the "Customer Acceptance Policy" the banker should take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner that banker is satisfied and it knows who the beneficial owner(s) is/are. An indicative list of the nature and type of documents that may be relied upon for customer identification is given in the Annexure II.

Monitoring of transaction: Ongoing monitoring is an essential element of effective KYC procedures, banks can effectively control and reduce their risks only if they have an understanding of the normal and reasonable activity of the customer so that they have no difficulty in identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the sensitivity of the account. Banks/ Branches should pay special attention to all complex, usually large transactions and patterns, which have no apparent economic or visible lawful purpose. For effective monitoring of A/c's the following threshold limits are being prescribed:

Nature of A/c	Threshold limit
S.B. A/c	Rs. 2.00 lacs
R.D. A/c	Rs. 1.00 lacs
F.D. A/c (in service-individuals and General customers)	Rs. Upto 5.00 lacs
F.D. A/c (Retired salary earners with terminal Benefits And general public at large)	Rs. 5.00 lacs
C/D account (Individuals)	Rs. 1.00 lacs
C/D account (firms)	Rs. 5.00 lacs
C/D account (Corporate)	Rs. 10.00 lacs
CD societies Primary	Rs. 5.00 lacs
CD Societies (State level/Apex level)	Rs. 10.00 lacs

Banks/Branches should stick to aforesaid threshold limits assigned to the aforesaid categories of customers and their accounts and pay particular attention to the transactions, which exceeds these limits. Transactions that exceed the amounts of cash inconsistent with the normal and expected activities of the customers should particularly attract the attention of the banks/branches.

Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being washed through the account. High-risk accounts have to be subjected to intensified monitoring. Every bank/branch should have indicators for such accounts, taking note of the background of the customer such as the country of origin, source of funds and the type of transactions involved and other risk factors. Bank/Branches should review and categorize accounts periodically and if need be apply enhanced due diligence measures. Banks/branches should also report to Head Office about any abnormal transactions/activity taking place in such accounts every fortnight. Banks/Branches should also ensure that transactions in the account are preserved and maintained as required in terms of section 12 of the PML Act 2002, be ensured that transactions of suspicious nature and or any other types

of transactions notified under section 12 of PML Act 2002 are reported to the appropriate law enforcement authority.

Banks/Branches should maintain proper record of all cash transactions (deposits and withdrawals) of Rs. 5.00 lacs and above and should report all Such transactions and those of dubious/suspicious nature to their controlling office / Head Office regularly on fortnightly basis.

5. **Risk Management:-**

- (i) Banks/branches should ensure that the KYC policy is implemented in spirit and word.
- (ii) Banks/branches should ensure adherence to appropriate KYC procedures covering proper management oversight and controls segregation of duties, training and other related matters are stuck to and responsibility should be explicitly allocated to the bank/branch staff for ensuring that bank's policies and procedures are implemented effectively.
- (iii) Banks/Branches should create risk profiles of their existing and new customers and apply various money laundering measures, keeping in view the risk involved in a transaction/account or banking/business relationship.
- (iv) It is crucial that staff concerned at banks/branch level should fully understand the rationale behind the KYC policies and try to improve consistently.

6. Customer Education: Implementation of KYC policy and procedures requires banks to demand certain information from customers which is of personal nature or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the bank staff, so as to create doubt and confusion regarding the motive and purpose of collecting such

information. Therefore, a need for banks / branches to prepare special folders / hand bills/pamphlets etc. so as to educate the customer about the objectives of the KYC-Programme's policy and procedure. The front desk staff of the banks/branches should be well versed with the

KYC Policy and procedure so as to handle such situation while dealing with customers.

Introduction of new technologies- ATM Cards (Automated Teller Machine-Cards)

- (1) Banks / branches should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity and take measures, if needed to prevent their use in money laundering schemes.
- (2) Special precaution should be taken when funds are transferred electronically and in executing services warrant / involvement of agents. Banks / Branches should ensure that all agents are subjected to KYC Policy and procedure in the right spirit.

KYC for the existing accounts: Banks/Branches have been advised by NABARD to apply KYC norms to all existing customers in a time bound manner and the revised guidelines will apply to all new customers as well Banks/Branches should apply the same to the existing customers on the basis of materiality and risk. However, transactions in existing accounts should be continuously monitored and any unusual activity in operation of the account should trigger a review of the customer due diligence (CDD) measures. Bank/Branches need to apply monetary limits to such accounts based on the nature and type of the account, it should however, be ensured that the existing accounts are subjected to minimum KYC standard which would establish the identity of the natural customer and those of the "beneficial owners". Banks/Branches

should also ensure that term/recurring deposit accounts or accounts of renewal nature are treated as new accounts at the time of renewal and subjected to revised KYC procedures.

Where the bank/branch is unable to apply appropriate KYC measures due to non-furnishing of information and/or non-cooperation by the customer, the bank branch should consider closing the account or terminating the banking/business relationship after notice to the customer explaining the reasons for taking such a decision. Such decisions should be taken at a senior level.

Q2
/

KYC-Know your Customer-Policy and procedure:**1 Customer identification, requirements-indicative-guidelines:**

There exists the possibility that trust/nominees or fiduciary accounts can be used to circumvent the customer identification procedures. Bank/Branches should determine whether the customer is acting on behalf of another person as trustee or guarantor through other intermediary. If so, banks should insist on receipt of satisfactory evidence of the identity of the intermediary persons on whose behalf they are acting, and also obtain details of the nature of the trust or other arrangements in opening an account for a trust, banks should take reasonable precautions to verify the identity of the trustees and of the trust, including any person settling assets into the trust, grantors, protectors, beneficiaries and signatories, should be identified when they are defined. In the case of a "foundation" steps should be taken to verify managers/directors and the beneficiaries, if defined.

2 Accounts of companies and firms: Banks/branches should be vigilant against business entities being used by individuals as a front for maintaining accounts. Banks / branches should examine the control structure of the entity. Determine the source of funds and identify the natural who have a controlling interest and who comprise the Management. These requirements should be moderated according to the perception e.g. in the case of public company it will not be necessary to identify all the share holders.

3 Client accounts opened by professional intermediaries: When the bank has knowledge or reason to believe that the client account opened by a professional intermediary of a single client, that client must be identified. Banks also maintain pooled accounts managed by lawyers/ accountants or

Stockbrokers for funds held on deposit or escrow for a range of clients. Where funds of intermediaries are not so mingled at the bank and there are sub-accounts each of them attributable to a beneficiary the beneficial owners must be identified. Where such funds are Co-Mingled at the bank, the bank should still look for the beneficial owners. Where the banks rely on the customer due diligence done by an intermediary, satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to control KYC requirements. It should be well understood that the ultimate responsibility of knowing the customer lies with the bankers.

- 4 Accounts of politically exposed persons (PEPs) residing outside India: Politically exposed persons are individuals who are or have been entrusted with prominent public functions, for the country, e.g. Head of states of governments, senior politicians, senior government /Judicial/military officers/executives of state owned corporations, important political party official etc. Banks should gather sufficient information about any person of this category intending to establish a relationship and check all the information available about the person in the public domain.
- 5 Banks/Branches should verify the identity of the person and seek information about the source before accepting the PEP as a customer. The decision to open an account for PEP should be taken at a senior level and should be clearly spelt out in customer acceptance policy. Banks/Branches should also subject such accounts to enhance CDD on an ongoing basis. The aforesaid norms should also be applied to the accounts of the family members or close relatives of the PEP.
- 6 Accounts of Non Face to Face customers: With the introduction of telephone and electronic banking increasingly, accounts are being

opened by banks for customers without the need for the customer to visit the bank/branch. In the cases of non face to face customers, apart from usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher certification of all documents presented should be insisted upon and, if necessary, additional documents should be asked for. In such cases, banks should also require the first payment to be effected through the customers account. In the case of cross border customers, there is additional need of matching the customer with the documentation and the bank may have to rely on third party certification/introduction. In such cases it should be ensured that third party is a regulated and supervised entity and had adequate KYC systems in place.

7 Correspondent Banking: Correspondent banking is the provision of banking services by one bank (the correspondent bank) to another (the respondent bank). These services may include cash / funds management, drawing arrangements for demand drafts, transfers, payable through accounts cheques, clearing etc.

(i) Banks / Branches should gather sufficient information to understand nature of business of the correspondent / respondent bank. Information on the other banks management activities, level of AML/CFT compliance purpose of opening of the account, identity of any third party entities that correspondent banking services, and regulatory supervisory framework in the correspondents/respondents counters special, relevance.

a. similarly, banks should try to ascertain from publicly available information whether the other banks/branches is subject to any money laundering or terrorist financing investigation or regulatory action.

b. Banks/Branches should not establish any relationships, without the approval of the board/chairman/Administrator.

i If you are acting as a correspondent bank: before effecting payments be satisfied and ensure that the respondent bank has verified the identity of the customers before access to the accounts and is undertaking due diligence on them. Also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

ii You should refuse to enter into a correspondent relationship with a "Shell Bank": i.e. A bank which has been incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group. Shell banks are not to operate in India.

iii Don't establish relationship with respondent foreign financial institutions-that permit their accounts to be used by shell banks.

iv Exercise utmost caution while continuing relationship with respondent banks located in countries with poor KYC standards and countries identified as non cooperative against money laundering and terrorist financing.

8 Ensure that respondent banks have money laundering policies and procedures in place and apply enhanced "Due Diligence" procedures for transactions through the correspondent accounts.





ANNEXURE II

Customer identification procedures:

Features that should be verified and documents that should be obtained from customers.

S.NO.	Features	Documents
1	Accounts of Individuals	
A	Legal name and any other names used	(I) Passport (II) PAN-CARD (III) Voters identity card (IV) Driving licence (V) Identity Card (VI) Letter from recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of the bank/branch. (VII) Telephone Bill. (VIII) Water Bill. (IX) Electricity Bill. (X) Bank Account Statement (XI) Ration Card (XII) Property document (XIII) Letter from employer (subject to satisfaction of the bank)
B	Correct permanent address	Any one document that provides customer information to the satisfaction of the bank will suffice.
2	Accounts of companies a. Name of Company	1. Certification of incorporation and memorandum and articles of association 2. Resolution of the Board of Directors to open an account and identification of




	<p>b. Principal place of business.</p> <p>c. Mailing address of the company.</p> <p>d. Telephone and FAX.</p>	<p>Those who have authority to operate the accounts.</p> <p>3 Power of attorney granted to it's managers/officers or employees to transact business on it's behalf.</p> <p>4 Copy of PAN allotment letter.</p> <p>5 Copy of the telephone Bill in the name of firm /partners.</p>
4	<p>Accounts of Partnership firms</p> <p>A. Legal Name</p> <p>B. Address</p> <p>C. Names of all partners and their addresses.</p> <p>D. Telephone nos of the firm and partners.</p>	<p>a. Registration certificate, if registered.</p> <p>b. Partnership deed.</p> <p>c. Power of attorney granted to a partner/employee of the firm to transact business on it's behalf.</p> <p>d. Any valid document identifying the partners and the persons holding the power of attorney and their address.</p> <p>e. Telephone Bill in the name of firm/partners.</p>
4	<p>Accounts of foundations/trusts and associations</p> <p>a. Name of trustees, settlers beneficiaries and signatories.</p> <p>b. Names and addresses of the</p>	<p>a. Certificate of registration, if registered</p> <p>b. Power of attorney to transact business on it's behalf.</p> <p>c. Any officially valid documents specifying the trustees, settlers, beneficiaries and those holding power of attorney granted to founders/managers/directors and their addresses.</p> <p>d. Resolution of the Managing Body of the</p>

	Founder, the managers/directors and beneficiaries. c. Telephone/FAX	Foundations/trusts/associations. e. Telephone Bills
--	------------------------------------------------------------------------	--------------------------------------------------------

Actions to be taken by the bank management at Head Office level:

- 1 Banks should appoint a senior Management officer to be designated as Principal Officer, Principal officer should be placed at Head/Corporate office of the bank and should be responsible for monitoring and reporting of all transactions and information as required under the law. He will maintain close liaison with enforcement agencies, banks and other institutions which are involved in the fight against money laundering and combating financing of terrorism.
- 2 Board of directors of the bank should ensure that an effective KYC programme is put in place by appropriate procedures and ensuring their effective implementation. It should cover proper management oversight and controls, segregation of duties, training and other related matters. Responsibilities should be explicitly allocated by the bank for ensuring that the banks policies and procedures are implemented effectively. Bank's in consultation with boards, should devise procedures for creating risk profiles of their existing and new customers and apply various money laundering measures keeping in view the risks involved in a transaction, accounts or banking/ business relationship.




Internal Audit: Bank Management should ensure that their audit cell is staffed adequately with individuals who are well-versed in such policies and procedures because banks internal audit and compliance functions have an important role in evaluating and ensuring adherence to policies and procedures. As a general rule, the compliance function should provide an independent evaluation of bank's own policies and procedures, including legal and regulatory requirements. Concurrent/Internal Auditors should specifically check and verify the application of KYC procedures at the branches and comments on the lapses observed in this regard. The compliance in this regard should be put up before the **Audit Committee of Board** on quarterly interval.

Training of Bank Staff: Bank's management at head office level should ensure that there is an ongoing employee-training programme so that the members of the staff are adequately trained in regard to procedures. Training requirements should have different focuses for frontline staff, compliance staff and staff dealing with customers, since implementation of policy and procedures is a crucial matter, Managements should ensure that all concerned should fully understand the rationale behind the KYC policy and procedures and improve upon themselves consistently.

The implementation of KYC policy and procedures requires banks to demand certain information from customers which is of personal nature or which has hitherto never been called for. This can sometime lead to a lot of questioning by the Branch Staff which can create a lot of doubt and suspicion in the minds of the customers towards the motive and purpose of collecting such information. The front desk staff should be specially trained to handle such situations while dealing with customers.

Customer Education: In regard to implementation of policies and procedures of the KYC a lot of questions / queries and information is to be given by the



Customer to the bank staff which may lead to a lot of confusion/ doubt at the customers level. In order to avoid such confusion/doubts etc. customers have to be educated regarding the KYC policies and procedures. For this purpose bank management should prepare and supply branches with special pamphlets/folders/Handbills etc.

Correspondent Banking: Correspondent banking is the provision of banking services by one bank (the "Correspondent Bank") to another (Respondent Bank). These services may include cash/funds managements, drawing arrangements for demands drafts transfers payable through accounts, cheques clearing etc. For this a relationship is to be established between two aforesaid banks, i.e. the correspondent bank and the respondent bank which should be established with the approval of the board in case the Board Wishes to delegate the power to an administrative authority, it may delegate the power to a committee headed by the Chairman/Administrator of the bank, while laying down clear parameters for approving such relationships. Proposals approved by the committee should invariably be put up to the board at it's next meeting for "Post Facto Approval".

Further resolved that all the provisions of "Know your customer policy"- Anti Money Laundering Act 2002, as and when revised by the RBI will automatically become part of the aforesaid policy, when circulated for implementation.


Managing Director


Administrator

