

POLICY ON KYC & AML

Sl. No.	TABLE OF contents CHAPTER
1.	Introduction-Objective of the Policy
2.	Customer Acceptance Policy (CAP)
3.	Customer Identification Procedure (CIP)
4.	Monitoring of Transactions
5.	Risk Management
6.	Training Programme
7.	Internal Control Systems
8.	Record Keeping
9.	Evaluation of KYC Guidelines
10.	Duties/ Responsibilities and Accountability

CHAPTER-I

INTRODUCTION

01.01. OBJECTIVE

The objective of **KNOW YOUR CUSTOMER (KYC)** guidelines is to prevent banks from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable banks to know/understand their customers and their financial dealings better, which in turn help them, manage their risks prudently.

<http://www.continuitycentral.com/newslettermanagement2.htm> The Basel Committee has highlighted the need for banks to implement effective 'know-your-customer' (KYC) standards as an essential part of risk management practices.

The committee states that banks with inadequate KYC risk management programme may be subject to significant risks, especially legal and reputational ones. Sound KYC policies and procedures not only contribute to a bank's overall safety and soundness, they also protect the integrity of the banking system by reducing the likelihood of banks becoming vehicles for money laundering, terrorist financing and other unlawful activities.

The Basel Committee also states that a key challenge in implementing sound KYC policies and procedures is how to put in place an effective approach. The legal and reputation risks are global in nature and as such, it is essential that each bank develops a global risk management programme supported by policies that incorporate KYC standards.

It is important that the adoption of customer acceptance policy and its implementation should not become too restrictive and must not result in denial of banking services to general public, especially to those, who are financially or socially disadvantaged.

The term 'Money laundering activities' cover not only the criminals who try to launder their ill-gotten gains, but also the bank/financial institutions and their employees who participate in their transactions and have knowledge that the property is criminally derived. "Knowledge" includes the concepts of conscious avoidance of knowledge. Thus, employees of a branch whose suspicions are aroused, but who then deliberately fail to make further inquiries/ report to higher authorities, wishing to remain ignorant, should be considered to have the requisite "knowledge" of criminal activities/transactions.

01.02. DEFINITION OF A CUSTOMER

For the purpose of KYC policy, a Customer may be defined as :

- a person or entity that maintains an account and/or has a business relationship with the bank 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, which can pose significant reputation or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

01.03. KYC policy includes the following nine key elements:

1. *Customer Acceptance Policy*
2. *Customer Identification Procedures*
3. *Monitoring of Transactions*
4. *Risk management*
5. *Training Programme*
6. *Internal Control Systems*
7. *Record Keeping*
8. *Evaluations of KYC guidelines by internal audit and inspection system*
9. *Duties / Responsibilities and Accountability.*

01.03.01. Implementation of instructions :-

While existing instructions of Reserve Bank of India would continue to be implemented, new provisions included in KYC guidelines are to be implemented with effect from 01.01.2005.

CHAPTER-II

CUSTOMER ACCEPTANCE POLICY (CAP)

As per RBI guidelines the Bank should develop a Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy enumerates explicit guidelines on the following aspects of customer relationship in the bank.

1. No account is opened in anonymous or fictitious/ benami name(s);
2. Not to open an account or close an existing account where the branch 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 bank.
3. It may, however, be necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision to close an account may be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.
4. Circumstances, in which a customer is permitted to act on behalf of another person/entity, should 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 may be opened by an intermediary in the fiduciary capacity and
5. Necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations available from Circulars etc.

02.01. Indicative Guidelines

02.01.01 Trust/Nominee or Fiduciary Accounts

Branch/offices should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, branch/offices may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place.

While opening an account for a trust, banks should take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories.

Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined. There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures.

02.01.02 Accounts of companies and firms

Branch/office need to be vigilant against business entities being used by individuals as a front for maintaining accounts with banks. Branch/office may 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.

02.01.03 Client accounts opened by professional intermediaries

When the Branch/office has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Branch/office may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Branch/office also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients.

Where funds held by the intermediaries are not co-mingled at the Branch/office and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the Branch/office, the bank should still look through to the beneficial owners. Where the Branch/office rely on the 'customer due diligence' (CDD) done by an intermediary, they should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. It should be understood that the ultimate responsibility for knowing the customer lies with the Branch/office.

02.01.04 Adherence to Foreign Contribution Regulation Act (FCRA), 1976

Branches/Offices should also adhere to the instructions on the provisions of the Foreign Contribution Regulation Act, 1976 cautioning them to open accounts or collect cheques only in favour of association, which are registered under the Act ibid by Government of India. A certificate to the effect that the association is registered with the Government of India should be obtained from the concerned associations at the time of opening of the account or collection of cheques. Branches/offices are advised to exercise due care to ensure compliance and desist from opening accounts in the name of banned organizations and those without requisite registration.

02.01.05 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. Branch/office 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.

Branch/office should verify the identify of the person and seek information about the sources of funds 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 subjected to monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs

02.01.06. Correspondent Banking

Relationships with correspondent banks should be established only with the approval of the Board. Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). These services may include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing, etc. Banks should gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank.

Information on the other bank's management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the correspondent's/respondent's country may be of special relevance.

Similarly, bank should try to ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action.

The responsibilities of the bank with which correspondent banking relationship is established should be clearly documented. In the case of payable-through-accounts, the correspondent bank should be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them. The correspondent bank should also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

Branches/Offices should refuse to enter into a correspondent relationship with a "shell bank" (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group). Shell banks are not permitted to operate in India. Branches/Offices should also guard against establishing relationships with respondent foreign financial institutions that permit their accounts to be used by shell banks.

All Branches/Offices should be extremely cautious while continuing relationships with respondent banks located in countries with poor KYC standards and countries identified as 'non-cooperative' in the fight against money laundering and terrorist financing. Branches/Offices should ensure that their respondent banks have anti money laundering policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

02.01.07 Profile based on categorisation

Branches/offices should 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.

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, may be categorised as low risk.

Illustrative examples of low risk customers could 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, 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. Enhanced due diligence measures are to be applied 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.

CHAPTER-III

Customer Identification Procedure (CIP)

03.01. Customer Identification Procedure is to be carried out at different stages i.e.

- 1) while establishing a banking relationship,
- 2) while carrying out a financial transaction ,
- 3) when the Branch/Office has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information.

Branch/offices need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship.

Being satisfied means that the Branch/office 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.

03.01.01. Natural Persons.

For customers that are natural persons, the Branch/office should obtain sufficient identification data to verify the identity of the customer, his address/location and also his recent photograph.

03.01.02. Legal Persons.

For customers that are legal persons or entities, the branch/office should 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.

If the branch/office decides to accept such accounts in terms of the Customer Acceptance Policy, the bank should take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are.

03.01.03. For New Accounts

"Know Your Customer" (KYC) procedure should be the key principle for identification of an individual/corporate opening an account. The customer identification should entail verification through an introductory reference from an existing account holder/a person known to the bank or on the basis of documents provided by the customer.

03.01.04. **Customer Identification:**

The objectives of the KYC framework should be two fold

1. to ensure appropriate customer identification and
2. to monitor transactions of a suspicious nature.

Banks should obtain all information necessary to establish the identity/legal existence of each new customer, based preferably on disclosures by customers themselves. Easy means of establishing identity would be documents such as passport, driving license, etc. Where such documents are not available, verification by existing account holders or introduction by a person known to the bank may suffice.

03.01.05. **Existing Accounts :**

With a view to ensuring that existing small account holders are not inconvenienced and the KYC procedures is completed in time, it has been decided that application of KYC procedures may be limited to the existing accounts, where the credit or debit summation for the financial year ended March 31, 2003 is more than Rs. 10.00 lakh or where the branch or office suspects any unusual transaction.(Refer Circular No.305/2004 dated 16.11.2004) however, branches/offices should fully implement the KYC norms in all existing accounts of trusts, companies/firms, religious/charitable organizations and other institutions or where the accounts are opened through a mandate or power of attorney.

03.01.06. **Introduction**

The customer identification will be through an introductory reference from an existing account holder/person known to the Bank and or on the basis of documents provided by the customer.

Introduction in Rural and Semi-Urban branches

The individuals in **rural and semi urban branches** can open deposit accounts by providing introduction from a third person having satisfactory conduct of the account for six months (barring new branches) or by well known local authorities or through staff members, against whom disciplinary proceedings are not pending, knowing the potential customer.

Introduction in Urban and Metro centre branches

In urban and metro centre branches, accounts to be opened on the basis of any one of the following.

An introduction from a third person having satisfactory conduct of the account for at least 12 months or by well known local authorities or through staff members knowing the potential customer.

Passport alone, may be accepted, when the address on the passport is the same as the address in the account opening form. Any other document from each of the under noted two lists for a photo ID and proof of residence.

	<i>List 1</i>		<i>List 2</i>
1.	Passport where the address differs	1.	Credit Card Statement**
2.	Election ID Card*	2.	Salary Slip**
3.	Pan Card*	3.	Income / Wealth Tax Assessment Order
4.	Govt./Defence ID Card	4.	Electricity Bill**
5.	ID Cards of reputed employers	5.	Telephone Bill**
6.	Driving License		

* With a self signed cheque drawn on existing bank. ** Latest/recent

Documents under List 1 will establish identity of the account holder and documents of List 2 will give present address of the account opener.

While the above set of documents should normally suffice to establish both the identity and the correct address of the applicant, wherever this is not so (e.g. PAN Card and Salary Slip together may not provide proof of address) applicants to be asked to give additional documents e.g. a letter from the employer giving the correct address, credit card statement etc. In case of joint account, applicants who are not closely related to each other would require to establish their identity and address independently.

In respect of NRI accounts, introduction and authentication/ verification of signatures to be made by a bank/Indian embassy/ Higher Commissioner/ Consulate/ Notary Public/ Persons known to the bank.

For establishing identity or proof of residence Ration Card should not be used as document. However, in the event of non-availability of any other document, Ration Card may also be accepted as proof of residence from minors/ illiterate persons who are unable to produce other documents.

03.01.07. Other than individual accounts

Accounts on behalf of the following customers to be opened by our branch/office after obtaining documents stated against their names and any other documents/ introduction that branch/office feel necessary to comply with KYC guidelines.

Company – Certificate of Incorporation, Memorandum and Articles of Association, Certificate of commencement of business where required and a copy of the resolution of the Board of Directors for opening of account.

Society/Associates/Clubs – Resolution for opening of the account and a copy of bye-laws and certificate of registration in case of registered clubs, societies and associations.

HUF – Declaration from the Karta.

Trust – A copy of the resolution, trust deed and a copy of registration certificate.

Firms – In the case of Partnership firm, partnership letter and introduction from a person known to the bank.

03.01.08. Letter of thanks –

In all instances of opening of new accounts letter of thanks to be sent by registered post at the recorded addresses to all customers and introducers with dual purpose, thanking them for opening the account with the Bank and for verification of genuineness of address furnished by the account holder. Undelivered envelopes in this regard would be required to be followed up closely at branch levels.

The operating staff/ officers associated with opening of accounts would be required to exercise due diligence and care at the time of opening of accounts. Care should, however, be taken that implementation of KYC guidelines do not result in denial of opening of new accounts.

03.02. Customer Profile

Care to be exercised that implementation of the KYC guidelines should not result in denial of opening of new accounts at the branches. Nevertheless, customer profiles to be compiled without exception.

For the purpose of exercising due diligence on individual transactions in accounts, 'Customer Profile' of individual account holders in the account should be incorporated in the opening forms, covering the following information :-

03.02.01. Mandatory Information to be included in the opening form :-

- 1) Occupation
- 2) Source of funds
- 3) Monthly Income
- 4) Annual turnover
- 5) Date of Birth
- 6) Dealings with other banks
- 7) Existing credit facilities

03.02.02 . The following information may be collected by the branch (which is Optional) for better customer relationship:-

1. Marital Status;
2. Educational Qualification;
3. Educational Qualification of spouse;
4. Details regarding children;
5. Information like -
 - a) Owns a car/two wheeler
 - b) have credit card
 - c) Have insurance policy.

03.02.03. Periodical Review of Customer Profile

The Customer profiles incorporated in the opening forms have to be reviewed once in three years.

03.02.04. The account opening form

For opening accounts by transfer from other branches, a new set of account opening forms along with the customer profile to be obtained.

While transferring accounts from inoperative accounts to live ledger, a new set of account opening form along with the customer profile to be obtained/ updated.

The prospective customer should not be insisted upon for the optional information. Wherever Bank desires to collect any information about the customer for the purpose other than KYC requirement, it should not form part of the account opening form. Such information may be collected separately, purely on a voluntary basis after explaining the objective to the customer and taking customers express approval for the specific uses to which such information could be put.

The aforesaid optional information may not be insisted upon from the existing customers. The information given in the Account Opening Form other than optional information, as mentioned above, are mandatory, as such branches must obtain the same so as to comply with the KYC guidelines.

Caution is to be exercised with regard to introduction of large number of accounts by a single introducer (either account holder or staff).

03.02.05 CHECK LIST

Features to be verified and documents that may be obtained from customers

Features	Documents
<p>Accounts of individuals</p> <p>Legal name and any other names used</p> <p>*Correct permanent address</p>	<p>Recent Photograph and (any one document which provides customer information to the satisfaction of the branch)</p> <p>Passport PAN card Voter's Identity Card Driving licence Identity card (subject to the bank's satisfaction)</p> <p>Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of branch/office Telephone bill Bank account statement Letter from any recognized public authority Electricity bill Ration card Letter from employer (subject to satisfaction of the branch)</p>
<p>Accounts of companies</p> <p>Name of the company</p>	<p>Certificate of incorporation and Memorandum & Articles of Association Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account</p>
<p>Principal place of business</p> <p>Mailing address of the company</p> <p>Telephone/Fax Number</p>	<p>Power of Attorney granted to its managers, officers or employees to transact business on its behalf Copy of PAN allotment letter Copy of the telephone bill</p>
<p>Accounts of partnership firms</p> <p>Legal name</p> <p>Address</p> <p>Names of all partners and their addresses</p> <p>Telephone numbers of the firm and partners</p>	<p>Registration certificate, if registered Partnership deed Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses Telephone bill in the name of firm/partners</p>
<p>Accounts of trusts & foundations</p> <p>Names of trustees, settlers, beneficiaries and signatories</p> <p>Names and addresses of the founder, the managers/directors and the beneficiaries</p> <p>Telephone/fax numbers</p>	<p>Certificate of registration, if registered Power of Attorney granted to transact business on its behalf Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/managers/ directors and their addresses Resolution of the managing body of the foundation/association Telephone bill</p>

CHAPTER-IV
Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. Branches 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 will depend on the risk sensitivity of the account.

04.01. High-risk accounts

Branches should pay special attention to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose.

The branch/office may prescribe threshold limits for a particular category of accounts 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 should particularly attract the attention of the bank. 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. Bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors.

04.01.01. Cash Transactions (Issue of DD/TT/MT/PO,etc.)

Banks are required to issue travelers cheques, demand drafts, mail transfers and telegraphic transfers for Rs.50,000 and above only by debit to customers accounts or against cheques and not against cash.

Applicants (whether customers or not) should furnish permanent (income tax) account number (PAN) on the application for issue of travelers cheques, demand drafts, mail transfers and telegraphic transfers if the amount exceeds Rs. 50,000.

In case customer/account holders not having PAN, since their income (from all sources) falls below the income tax exemption limit, the procedures to be adopted is mentioned below.

04.01.02 For PAN – under noted procedure to be followed :

Category of Customer

Procedure adopted

- | | |
|--|---|
| 1. Account holders having PAN and recorded with Bank | A suitable provision is available in the Draft/TT/Bankers order/RTC application form for affixing PAN under the signature of the account holder. |
| 2. Account holders not having PAN since their income (from all sources) falls below the Income Tax exemption limit | A declaration on Form No. 60 of I.T.Rules be obtained (form being obtained to open the new accounts from the customers not having the PAN). The declaration is to be obtained along with the application form. The account holder should sign the declaration to be printed <u>on the reverse of the application form.</u> |
| 3. Account holders not allotted PAN even though applied for it (holding acknowledgement for application) but their income is assessed for Income Tax and Assessment order issued by appropriate authority. | A declaration on Form No. 60 of I.T.Rules be obtained. The account holder should give a suitable statement in the form. The official in charge of the drafts business at the branch should act diligently and satisfy himself about genuineness of the statement. |
| 4. Account holders who have agricultural income and is not in receipt of any other income chargeable to Income Tax. | A declaration on Form No. 61 of I.T.Rules be obtained (as this is the form permitted to open the new accounts for a person who has agricultural income and is not in receipt of any other income chargeable to Income Tax for not having the PAN). The declaration is printed on the reverse of the application form. The account holder should sign the declaration printed <u>on the reverse of the application form.</u> |
| 5. Account holder whose income is neither assessed for IT nor applied for PAN and not fall under any of the category (1) to (4) above. | The account holders will be advised to obtain the PAN and his application for purchase of DD./TT/BO/RTCs for Rs.50,000/- and above be rejected politely. |

Further income tax Act and Rules require obtention of PAN only in cash purchase of bank drafts/pay orders/bankers cheque aggregating Rs. 50,000/- or more during any one day from a banking company (branch).

Branches/Offices should ensure that a record of transactions in the accounts is preserved and maintained as required in terms of section 12 of the Prevention of Money Laundering (PML) Act, 2002, wherein it is stated that the Banking companies, financial institutions, intermediaries and their officers shall not be liable to any civil proceedings against them for furnishing information under the Act.

It may also be ensured that transactions of suspicious nature and/ or any other type of transaction notified under section 12 of the PML Act, 2002, is reported to the appropriate law enforcement authority.

Branches are required to report all cash deposits and withdrawals of Rs.10 lakh and above as well as transactions of suspicious nature with full details in fortnightly statements to their respective zonal offices. Zonal offices are also required to appraise the Head office regarding transactions of suspicious nature.

04.02. PROCESS AND PROCEDURES TO MONITOR SUSPICIOUS TRANSACTIONS

Branches are required to record and report all transactions of suspicious nature in deposit, loan and remittance accounts etc, with full details to their controller/Zonal Offices

04.02.01. Transactions of suspicious nature

The procedure to be followed is as under -

The Principal officer/Officer -in charge, vested with the authority to open the account, is to ensure compliance with the KYC guidelines. The employee/officer, who has interviewed the customer's to subscribe his signature for having interviewed the prospective customer and the officer, before permitting opening of the account, to satisfy that all aspects of KYC guidelines are complied with.

In cash transactions RBI guidelines are required to be strictly complied with and a close watch of individual cash withdrawals and deposit for Rs.10.00 lac and above in deposit, cash credit or overdraft accounts and recording of the transactions in a separate register is to be done.

Threshold limit of transaction

At the time of opening of the account, based on customer's profile, a threshold limit of transaction is to be determined. To begin with all transactions up to Rs. 10.00 lac

will be exempted from the purview of the scrutiny. Further; it is proposed to have a threshold limit of Rs.50000/- in case of individuals; one month turnover in the case of business enterprise (including business professionals) or Rs. 10.00 lac wherever is lower. These limits are to be reviewed and revised on yearly basis or as requested by the customer from time to time and any transaction beyond this limit should be looked into with extra caution.

Activity monitoring to cover all accounts including existing accounts for which profile to be made over a period of time. Branch Managers should use reasonable judgment in determining the suspiciousness of the transaction and the accounts wherein the suspicious transactions were found are to be closely monitored at the branches, so that the documentary evidence upon which a suspicion is aroused is not lost.

A courteous approach in the process is very essential to take care that the customers are not driven away from the Bank.

04.02.02. Reporting system for high value cash/suspicious transaction

04.02.03. Cash transaction of Rs. 10.00 lac and above

Branches are required to record and report all individual cash deposits and withdrawals of Rs. 10.00 lac and above in deposits, cash credit and overdraft accounts etc, at fortnightly intervals to the respective Zonal Offices.

Suspicious Transactions

To observe four eyes concept in reporting suspicious transactions at branch level, first dealing officer at the branch will report to the Branch Manager (BM), who will get himself satisfied about existence of a suspicious activity/nature and then report to the Zonal office. Further course of action is to be recommended by the Zonal Manager in consultation with Law Department to H.O. The designated officer at H.O has to take up the matter with appropriate law enforcing authorities designated under the relevant laws governing such activities.

The Zonal Manager/Controlling Authority during their visit/surprise inspection to Branch, have to verify the account opening forms/transactions recorded in the register for the purpose at random.

Zonal Office should submit the particulars of such incidents reported and the action initiated against them in a prescribed format to PMD Dept. (H.O.) at quarterly intervals.

04.02.04 Terrorist finance

Incase the name of any banned organization is noticed as payee/endorsee/applicant, the first dealing officer shall report the same to the Principal Officer. Reporting of such transactions as and when detected is to be done as under:

<i>Reporting by</i>	<i>Reporting to</i>
<i>1. Branch</i>	<i>1. Zonal Office/Controller</i>
<i>2. Zonal Office/Controller</i>	<i>2. PMD. H.O.</i>
<i>3.PMD. H.O</i>	<i>3.RBI (till RBI/Govt. Identifies appropriate authority)</i>

Annexure - I

Transaction of suspicious nature

(I) Transactions not consistent with customer's business

1. Frequent withdrawals in cash by corporate customers, instead of cheque transactions without giving cogent reasons.
2. Customers insisting on cash payment of cheques drawn in the name of the firm without routing through their account, quoting reason for pressing payment of outstanding dues.
3. High value deposits routed through newly opened accounts and gradual cash withdrawals leaving small balances.
4. A single substantial cash deposit composed of many high denomination notes.
5. Instruments with multiple endorsements.
6. Accounts where large volume of credits through DD/TT/BC whereas the nature of business does not justify such credits.
7. Frequent exchange of small denomination notes for large denomination notes and vice versa in large quantities.
8. Frequent credits in cash into the account by person other than the account holder or his authorized representative.

(II) Attempt to avoid reporting/ circumventing prescribed guidelines

Frequent issue of demand drafts/banker's cheques / telegraphic transfers for sums deposited in cash just below threshold limit of Rs.50,000/- thereby not routing the transaction through the account. Intentional splitting of transactions into small amounts to avoid reporting of transaction which may become necessary in case the threshold limit is crossed

Requesting Bank to open multiple accounts with a view to circumvent reporting by the Bank as per existing regulations.

Frequent opening and closing of accounts in short duration of time with a view to avoiding reporting of transactions involved as per existing regulations.

(iii) Unusual activities

1. Opening of account at places away from place of work/residence of the individual/firm.
2. Frequent operations in safe deposit lockers followed by cash deposits especially deposits just under the threshold levels.
3. Frequent deposit of large sums of money bearing labels of other banks into the accounts.
4. Request for closure of newly opened accounts where high value transactions have been routed through them and funds withdrawn immediately.

(iv) Customers who provide insufficient or suspicious information

1. Reluctance of the customer/corporate to furnish details about their activities or providing financial statements.
2. A customer who has no record of past or present employment but makes frequent large transactions through the account.
3. Letter of thanks sent to the customer/introducer returned undelivered.

(v) Certain Bank employees arousing suspicion

1. Unexplained shortages of significant amount of Bank's funds reported on account of the same employee(s).
2. Reluctance to take job rotation/routine transfer.
3. Employee does not avail leave/vacation.
4. Negligence of employee's willful blindness is reported repeatedly.
5. Life-style of the employee inconsistent with the known sources of income.
6. Frequently exceeding the discretionary power and allowing excess drawings to borrowers without proper justification/reporting to appropriate authority for control.
7. Request for frequent DD purchases of high value instruments by staff members.

Some examples of suspicious activities/ transactions to be monitored by the operation staff

- Large cash transactions.
- Multiple accounts under the same name.
- Frequently converting large amounts of currency from small to large denomination notes.
- Placing funds in term deposits and using them as security for more loans.
- Large deposits immediately followed by wire transfers.
- Sudden surge in activity level.
- Same funds being moved repeatedly among several accounts.
- Multiple deposits of money orders, Banker's cheques, drafts of third parties etc.
- Transactions inconsistent with the purpose of the account.
- Maintaining a low or overdrawn balance with high activity.

Note

1. The above list is illustrative and not exhaustive. The Principal Officer of the Branch/Office where suspicious activity/transaction is reported should verify the report depending upon the circumstances of the activity/ transaction reported and satisfy himself whether the activity/ transaction is to be reported as a suspicious activity/ transaction or is to be treated as a bonafide one. Care should be taken that the customers with bonafide transactions are not inconvenienced.
2. Activity monitoring should cover all accounts including existing accounts for which profiles have not been made.

CHAPTER-V

Risk Management

An effective KYC programme should be put in place by establishing appropriate procedures and ensuring their effective implementation. It should cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility should be explicitly allocated within the bank for ensuring that the bank's policies and procedures are implemented effectively.

The nature and extent of due diligence will depend on the risk perceived by the bank. 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 a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

Bank's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. The compliance function should provide an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. It should be ensured that the audit machinery is staffed adequately with individuals who are well versed in such policies and procedures.

Internal Inspectors should specifically check and verify the application of KYC procedures at the branches/offices and comment on the lapses observed in this regard.

The compliance in this regard may be put up before the Audit Committee of the Board by HO (Inspection) on quarterly intervals.

CHAPTER-VI

Training Programme

Training of staff and management

A regular session should be conducted in all the training programmes of Staff Training College to equip the staff members on 'KYC' & 'AML' policy so as to protect the Bank from money laundering activities.

Records to be kept of all formal training conducted. These records have to include the names and other relevant details, dates and locations of the training.

CUSTOMER EDUCATION

The front desk staff needs to be specially trained to educate the customers regarding the objectives of the KYC programme..

CHAPTER-VII

Internal Control Systems

Duties and responsibilities should be explicitly allocated for ensuring that policies and procedures are managed effectively and that there is full commitment and compliance to an effective KYC programme in respect of both existing and prospective deposit accounts.

Zonal offices should periodically monitor strict adherence to the laid down policies and procedures by the officials at the branch level.

CHAPTER-VIII

Record Keeping

Branch/offices should prepare and maintain documentation on their customer relationships and transactions to meet the requirements of relevant laws and regulations, to enable any transaction effected through them to be reconstructed.

In the case of wire transfer transactions, the records of electronic payments and messages must be treated in the same way as other records in support of entries in the account.

Retention of Records

In terms of the Banking Regulation Act, records such as Account Opening Forms, vouchers, ledgers, registers, etc pertaining to Banking Transactions for specified periods are required to be maintained. In addition, the following documents in respect of accounts, which have been reported for suspicious activities, are required to be retained at the end of business relationship with the customer, which in any case shall not be less than 5 years.

1. Customer Profiles
2. Reports made to government authorities concerning suspicious customer activities relating to possible money laundering or other criminal conduct together with supporting documentation.
3. Records of all formal anti money laundering training conducted which include the names and business units of attendees and dates and locations of the training; and
4. Any other document required to be retained under applicable money laundering laws/regulations.

All financial transactions records are to be retained at least for 5 years after the transaction has taken place and to be made available for scrutiny of Law enforcing agencies, Audit functionaries as well as Regulators as and when required.

CHAPTER-IX

Evaluations of KYC guidelines by internal audit and inspection system

An independent evaluation of KYC guidelines for identifying high value transactions would require to be carried out by Concurrent/Internal Auditors. They would be required to comment on the effectiveness of measures taken by branches/level of implementation of KYC guidelines and prevention of money laundering at branches/Offices.

A review of the compliance with KYC guidelines at branches in this regard will be put up by Inspection and Audit Department to the Audit Committee of the Board at quarterly intervals along with quarterly review being put up now covering inspection and audit and concurrent audit, etc. for the whole Bank.

Further, Concurrent / Internal auditors should specifically scrutinize and comment on the effectiveness of the measures taken by branches in adoption of KYC norms and steps taken by the branch towards prevention of money laundering.

CHAPTER-X

DUTIES/ RESPONSIBILITIES AND ACCOUNTABILITY

The importance of KYC guidelines to the employees

The Bank employees will conduct themselves in accordance with the highest ethical standards and in accordance with the extant regulatory requirements and laws. Staff and management shall not provide advice or other assistance to individuals who are indulging in money laundering activities. The chain of duties and responsibilities at branches/ controlling offices and accountability are as under and non-compliance of the duties and responsibilities arising out of KYC guidelines will lead to fixation of accountability. Dereliction of duty and avoidance of knowledge will lead to examination of staff accountability.

<i>Personnel</i>	<i>Duties/Responsibilities</i>
Officer in Charge of accounts/ Officer vested with the authority to open new accounts	To interview the potential customer To verify the introductory reference/ customer profile To arrive at threshold limits for each account (new as well as existing) and to exercise due diligence in identifying suspicious transactions. To ensure against opening of accounts in the names of terrorist/ banned organizations To adhere to the provisions of Foreign Contribution Regulatory Act 1976. To comply with the guidelines issued by the Bank from time to time in respect of opening and conduct of account.
Principal Officer	To scrutinize and satisfy himself/herself the information furnished in the account opening form/customer profile/threshold limit are in strict compliance with KYC guidelines before authorizing opening of account. To certify in the Statement /Register regarding compliance with KYC guidelines and report suspicious transactions to appropriate authority.
Concurrent Auditor whenever posted	To verify and record his comments on the effectiveness of measures taken by branches/level of implementation of KYC guidelines
Controlling Authority	Prompt reporting of information regarding suspicious transactions to the law enforcing authority concerned in consultation with Planning &Marketing Dept., Head Office

